Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 07 – 2023
REVISTA ONLINE, Anual

Direção Executiva
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

Data: 2023

Publicação: anual

ESTATUTO EDITORIAL

1.º Objeto. A Revista Privacy and Data Protection Magazine é uma publicação científica que tem por objeto a Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual; Direito do Consumo; Direito da Saúde, Direito Digital e Inteligência Artificial.

2.º Princípios Deontológicos. Tudo o que, nesta Revista, se venha a publicar, obedecerá rigorosamente à metodologia científica do Direito e à sua praxis quotidiana, sem quaisquer ingredientes políticos ou religiosos. Assim, será sempre no respeito dos princípios deontológicos da imprensa periódica e da ética profissional que se pautará a orientação desta Revista.

3.º Propriedade. É proprietária da Revista a ENSILIS – Educação e Formação, Unipessoal Lda, detentora da Universidade Europeia, com sede na Quinta do Bom Nome, Estrada da Correia, n.º 53, 1500-210.

4.º Edição. A edição da Revista está a cargo da Universidade Europeia.

5.º Objetivo. A Revista visa contribuir para a criação e transmissão do conhecimento científico na área da Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

6.º Direção Executiva e Editorial. A Revista é dirigida por uma diretora: Cristina Maria de Gouveia Caldeira, que é co-coordenadora do Privacy and Data Protection Centre, email: centro.dataprotection@universidadeeuropeia.pt

7.º Colaborações. A Revista publica em acesso aberto artigos doutrinários e outros estudos, legislação e jurisprudência comentadas e recensões de obras científicas.

8.º Conselho Editorial. Após revisão por pares, a seleção dos trabalhos a publicar é feita por um Conselho Editorial integrados por 6 especialistas de reconhecido mérito.

9.º Periodicidade. A Revista terá periodicidade quadrimestral.

10.º Secções. A Revista compreende quatro secções: (i) Artigos Doutrinários; (ii) Outros Estudos; (iii) Legislação e Jurisprudência Comentadas; (iv) Recensões.

11.º Sistema de Publicação. A Revista com publicação online em três línguas (português, inglês e espanhol), pretende ter um alcance nacional e internacional.

Ficha Técnica

Título
Privacy and Data Protection Magazine

Subtítulo
Revista Científica na Área Jurídica

Número
007

Ano de Publicação
2023

Afiliação
Privacy and Data Protection Centre Universidade Europeia

Autores
Alexandre Sousa Pinheiro
Cristina Maria de Gouveia Caldeira
Diana Camões
Débora de A. M. dos Santos Martins
D'joline Bragança Augusto
Duarte Rodrigues Nunes
Isabel Celeste M. Fonseca
Joana Maria de Oliveira Moreira
Joel A. Alves
Leonel do Rosário Filipe Salgueiro
Manuel David Masseno
Marcilete Cardoso da Silva
Mateus Silva Rocha
Paulo Alexandre D.S.C. Teles
Renata Guilardi de Oliveira Castro

Prefácio
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Direção Executiva
Cristina Maria de Gouveia Caldeira

ISSN
2184-920X

Número de Registo
127600

Propriedade
ENSILIS - Educação e Formação, Unipessoal, Lda., detida a 100% por Omnymission, Unip. Lda.

Chief Executive Officer
Carlos Bertrán

NIPC/NIF
504 669 788

Editor e Redação
Universidade Europeia, Quinta do Bom Nome, Estrada da Correia, 53, 1500-210, Lisboa

Universidade Europeia

Índice

Prefácio

A revista *Privacy and Data Protection Magazine* não é alheia às mudanças e aos novos desafios que se colocam à investigação e ao ensino superior, contribuindo para o aprofundamento da doutrina jurídica e reafirmando o compromisso de publicar artigos relevantes na área do Direito e em área afins.

Com uma publicação anual a partir de 2023, em acesso aberto, constitui-se como um veículo de difusão de novos conhecimentos para investigadores, professores e estudantes, de várias áreas científicas, mas sobretudo de grande proximidade às temáticas que irão ser estudadas no âmbito do novo Mestrado em Direito e Segurança da Informação, da Universidade Europeia, em regime de ensino a distância, com início a partir de outubro de 2024.

Na sua parte doutrinária, a presente publicação versa sobre temáticas centrais do ponto de vista de uma problematização da governação e da reutilização de dados sob custódia da Administração Pública, dando especial atenção à proteção de dados pessoais na legislação portuguesa e no Direito da União Europeia. O poder autárquico e os desafios que enfrenta com a (re)publicação na Internet das atas de reuniões dos seus órgãos colegiais remetem-nos para o regime-geral do acesso a documentos administrativos (LADA).

Com relevância teorética e dogmática, discute-se a viabilidade de enquadrar os ataques de *ransomware* no crime de "Fraude [Burla] informática", alargando a criminalização de atos contra o património praticados através de meios informáticos. Na referida parte da publicação, são ainda abordados tópicos centrais como a Lei da Comunicação eletrónica e a proteção de dados, as tecnologias emergentes aplicadas na área da saúde e os metadados, implicando a questão de saber se a conservação e o acesso das autoridades a esses dados restringem de forma intensa os direitos tutelados pelo Direito europeu e nacional. A matéria juscriminal da legalidade do acesso a registo e a dados cadastrais, no âmbito de investigações criminais, antecede um estudo constitucional comparado entre Portugal e o Brasil sobre a privacidade. Os desafios que se colocam ao constitucionalismo digital e à regulação da internet encerram os conteúdos doutrinários.

Em sede de "outros estudos", são acolhidas reflexões críticas sobre a separação de poderes, o ativismo judicial e a judicialização da Política, as impugnações das decisões judiciais e a relação do juiz com a política. Encerramos

esta outra parte da revista com uma alusão aos Direitos Fundamentais, em especial o direito à educação e a proteção dos dados pessoais.

A secção sobre "Legislação e Jurisprudência Comentadas" abre-se a dois acórdãos do Tribunal de Justiça da União Europeia.

Pela relevância e atualidade do tema, apresenta-se a recenção da obra "Privacidade e Proteção de Dados do Município de Lisboa", edição da Imprensa Municipal, de 2024, uma obra de natureza teórico-prática, uma referência nos domínios da privacidade, proteção de dados, inteligência artificial e governação de dados, que nos ajudará a trilhar os desafios que o cumprimento das normas de proteção de dados nos coloca.

Um profundo agradecimento a todos os que permitiram a publicaçação da PDPM de 2023, destacando em especial a colaboração da Dra. Renata Castro.

Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

I
Artigos Doutrinários

A governação e a reutilização de dados contidos em documentos administrativos e a proteção de dados pessoais na legislação portuguesa e no Direito da União Europeia

Alexandre Sousa Pinheiro[1]

Resumo
O presente texto baseia-se na evolução do mercado de dados europeu, no contexto de uma estratégia de dados da UE. Neste contexto, identificamos as fontes normativas europeias e nacionais relevantes para compreender o conceito de reutilização perante dados pessoais ou dados não pessoais. A aplicação do RGPD e a sua conciliação com as diversas formas de extrair informação constitui uma base essencial do trabalho. Compete avaliar os serviços de intermediação de dados e os seus conceitos naturais.

Palavras-chave: Proteção de dados pessoais; Proteção de dados não pessoais, reutilização de dados; dados abertos; serviço de intermediação de dados; partilha de dados; utentes de dados e detentores de dados.

[1] Professor Auxiliar da Universidade Europeia. Membro da CADA.

Governance and reuse of data contained in administrative documents and the protection of personal data in Portuguese legislation and European Union Law

Abstract
This text is based on the evolution of the European data market, in the context of an EU data strategy. In this context, we identify the relevant European and national normative sources to understand the concept of reuse when dealing with personal data or non-personal data. The application of the GDPR and its reconciliation with the different ways of extracting information constitutes an essential basis of the work. It is responsible for evaluating data intermediation services and their natural concepts.

Kewwords: Protection of personal data; Protection of non-personal data, data reuse; open data; data intermediation service; data sharing; data users and data holders.

1. Enquadramento das fontes

1.1. Origem e desenvolvimento normativo

Apesar de a Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do sector público,[2] ser indicada como instrumento jurídico fundador da regulação da matéria na União Europeia, deve considerar-se a influência de outros instrumentos normativos, como a Diretiva do Conselho 90/313/CEE, de 7 de junho de 1990, relativa à liberdade de acesso à informação em matéria de ambiente.

A própria Diretiva de 2003 faz referência no Considerando (2) à Diretiva 90/313/CEE:

> "(…) relativa à liberdade de acesso à informação em matéria de ambiente iniciou um processo de mudança na forma como as entidades públicas abordam a questão da abertura e da transparência, estabelecendo medidas para o exercício do direito de acesso do público à informação sobre ambiente, que deve ser impulsionado e prosseguido."

A Diretiva 90/313/CEE foi revogada pela Diretiva de 2003, não só para ampliar ao acesso à informação administrativa, como, também, para eliminar as disparidades existentes no acesso à informação entre os diversos Estados-Membros.

1.2. Os aspetos que merecem especial atenção previstos na Diretiva 2003/98/CE, e que influenciaram a futura legislação da UE sobre o acesso e tratamento da informação administrativa respeitam, nomeadamente, aos seguintes aspetos:

i) Previsão do princípio geral da reutilização dos documentos na posse do sector público, garante a reutilização de documentos na posse de organismos do sector público, sempre que permitida, e a disponibilização da informação através de meios eletrónicos (artigo 3.º);

ii) Ausência de os Estados-Membros autorizarem a reutilização de documentos e não continha regulação sobre o direito de acesso a documentos administrativos, que alterasse a legislação nacional (Considerando 9);

[2] Transposta para o Direito português pela Lei n.º 46/2007, de 24 de agosto, revogada pela Lei n.º 26/2016, de 22 de agosto, a atual Lei de Acesso aos Documentos Administrativos – LADA, onde permanece a transposição, com alterações posteriores.

iii) Disponibilização dos documentos em qualquer formato ou linguagem que já existam, sempre que possível e adequado, preferencialmente através de meios eletrónicos (artigo 5.º, n.º 1);

iv) Os emolumentos não poderiam exceder o custo da sua recolha, produção, reprodução e divulgação, acrescido de uma rentabilidade razoável para o investimento (artigo 6.º);

v) As condições aplicáveis à reutilização de documentos não deviam ser discriminatórias para categorias de reutilização equivalentes (artigo 10.º, n.º 1);

vi) A Diretiva de 2003, devia ser aplicada e executada cumprindo a Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Considerando 21);

vii) Os direitos de propriedade intelectual de terceiros não seriam afetados pela Diretiva, bem como os direitos de propriedade industrial (Considerando 22).

1.2.1. A Diretiva de 2003 foi alterada pela Diretiva 2013/37/EU de 26 de junho de 2013, enunciando-se como explicação geral da modificação que o regime jurídico de 2003 já estava superado pela evolução tecnológica, existindo "o risco de se perderem as oportunidades económicas e sociais proporcionadas pela reutilização dos dados públicos" (Considerando 5).

As alterações fundamentais introduzidas pela Diretiva de 2013, basearam-se em um sistema de "reutilização regra", salvas as exceções legislativamente previstas e tendendo a adquirir um caráter restritivo.

O princípio geral do artigo 3.º deixa de fazer depender a reutilização de normas permissivas, antes estabelece a regra de que os Estados Membros devem assegurar que os documentos a que se refere a Diretiva são reutilizáveis para fins comerciais ou não comerciais, salvo normas excecionais[3].

[3] "Considerando (8) A Diretiva 2003/98/CE deverá ser alterada de modo a estabelecer claramente a obrigação, para os Estados-Membros, de tornar reutilizáveis todos os documentos, exceto se o acesso for restrito ou vedado ao abrigo de regras nacionais sobre acesso a documentos e sem prejuízo das outras exceções previstas na presente diretiva. As alterações introduzidas pela presente diretiva não visam definir ou alterar regimes de acesso nos Estados-Membros, os quais continuam a ser da sua responsabilidade."

Na alteração ao artigo 4.º, n.º 4 da Diretiva de 2003, inseriram-se vias de recurso, em caso de indeferimento, após solicitação de reutilização de informação administrativa, que podem ter a natureza de organismo imparcial de recurso, de autoridade nacional da concorrência, de autoridade nacional de acesso a documentos ou uma autoridade judicial nacional[4].

A transposição da Diretiva de 2013 para o ordenamento jurídico português, atribuiu a competência para receber queixas à Comissão de Acesso aos Documentos Administrativos (CADA) prevista no artigo 22.º, n.º 1, alínea b) da LADA. Foram aprovadas, também, alterações que aqui não analisaremos, respeitando a formatos e a emolumentos.

Relevam também, no tema que tratamos, os seguintes Pareceres do Grupo de Trabalho do artigo 29.º: (i) Parecer n.º 3/99, sobre preservação de dados de tráfico de ISPs para finalidades de *law enforcement*[5] ; (ii) Parecer n.º 5/2001, sobre o Relatório Especial do Provedor de Justiça Europeu ao Parlamento Europeu na sequência do projeto de recomendação à Comissão Europeia relativo à reclamação 713/98/IJH[6] ; (iii) Parecer n.º 7/2003[7], sobre a reutilização da informação do sector público e proteção dos dados pessoais.

---

[4] "Considerando (28) Esse organismo deverá ser organizado de acordo com os sistemas constitucionais e legais dos Estados-Membros e não deverá prejudicar quaisquer vias de recurso distintas de que os requerentes de reutilização dispõem. No entanto, esse organismo deverá ser diferente do mecanismo do Estado-Membro que estabelece os critérios para cobrar emolumentos superiores aos custos marginais."

[5] Grupo de Trabalho do artigo 29.º, 5085/99/EN/FINAL WP 25, 7 de setembro de 1999.

[6] Grupo de Trabalho do artigo 29.º, 5003/00/EN/Final WP 44, 17 de maio de 2001.

[7] Grupo de Trabalho do artigo 29.º, 10936/03/PT WP 83, 12 de dezembro de 2003.

De acordo com as conclusões do Parecer: "A questão de saber se a diretiva [Diretiva 95/46/CE] sobre proteção de dados autoriza a reutilização de informação proveniente do sector público que inclui dados pessoais carece de uma avaliação cuidadosa e casuística que permita estabelecer um equilíbrio entre o direito à proteção da vida privada e o direito de acesso público. Os organismos do sector público terão que considerar a legitimidade da comunicação relativamente a cada caso concreto, de acordo com os critérios fixados na diretiva. Dado que a análise do princípio de finalidades é crucial neste contexto, o presente parecer apresenta vários elementos que terão que ser considerados nessa análise. Caso a comunicação seja prevista, os organismos do sector público terão que observar os direitos das pessoas em causa, como o direito de informação ou de oposição, em particular se os dados se destinarem a ser reutilizados para fins comerciais, como o marketing direto, por exemplo".

Esta posição do Grupo do Artigo 29.º não refere expressamente o consentimento (também não o exclui, evidentemente), admitindo outras fontes de legitimidade. O princípio da finalidade constitui a limitação fundamental da reutilização de documentos administrativos que contenham dados pessoais.

1.2.2. A Diretiva 2019/1024 de 20 de junho de 2019, transposta pela Lei n.º 68/2021, de 26 de agosto[8] , e que se integra na LADA (artigo 1.º, n.º 2) revogou a Diretiva 2003/98/CE[9], com a última redação com efeitos a partir de 17 de julho de 2021 (artigo 19.º) e introduziu importantes modificações no tema da reutilização tal como o estamos a tratar.[10]Algumas destas alterações extraem-se, nomeadamente, do Considerando (4):

(i) Disponibilização de acesso a dados dinâmicos em tempo real;

(ii) Permitir a reutilização de dados de empresas públicas[11], de organismos que realizam investigação e de organismos financiadores de investigação;

(iii) Evitar novos acordos de exclusividade.

Os dados dinâmicos previstos no artigo 2.º, n.º 8, da Diretiva, são transpostos para o Direito português no artigo 3.º, alínea k) da LADA:

> «"Dados dinâmicos", documentos ou dados em formato digital, sujeitos a atualizações frequentes ou em tempo real, em particular devido à sua volatilidade ou rápida obsolescência, como os dados gerados por sensores.»

---

[8] Com Declaração de Retificação n.º 31/2021, de 20 de setembro, publicado no DRE (Série I), de 26 de agosto de 2021.

[9] É igualmente revogada a Diretiva 2013/37 (artigo 19.º conjugado com o Anexo II).

[10] No Considerando (8) é apresentado o enquadramento da Diretiva: "O setor público dos Estados-Membros recolhe, produz, reproduz e divulga um largo espectro de informações em muitas áreas de atividade, como informações sociais, políticas, económicas, jurídicas, geográficas, ambientais, meteorológicas, sismológicas, turísticas, empresariais e sobre patentes e educacionais. Os documentos produzidos pelos organismos do setor público de natureza executiva, legislativa ou judicial constituem um conjunto de recursos vasto, variado e valioso que pode beneficiar a sociedade. A disponibilização dessas informações, o que inclui os dados dinâmicos, num formato eletrónico comum permite que os cidadãos e as entidades jurídicas encontrem novas maneiras de as utilizar e criem novos produtos e serviços inovadores. Nos seus esforços para tornar os dados facilmente disponíveis para reutilização, os Estados-Membros e os organismos do setor público podem ter a possibilidade de beneficiar de apoio financeiro adequado dos fundos e programas pertinentes da União e de receber esse apoio, assegurando uma ampla utilização de tecnologias digitais ou a transformação digital da administração pública e dos serviços públicos."

[11] "(Considerando 20) As empresas públicas recolhem, produzem, reproduzem e divulgam documentos para prestar serviços de interesse geral. A utilização de tais documentos para outros fins constitui uma reutilização. As políticas dos Estados-Membros podem ir além das normas mínimas estabelecidas na presente diretiva, permitindo assim uma reutilização mais alargada. Ao transporem a presente diretiva, os Estados-Membros poderão utilizar outros termos que não o termo «documentos», desde que mantenham integralmente o âmbito de aplicação do que é abrangido pela definição do termo «documento» na presente diretiva."

Os dados dinâmicos, levando em conta o Considerando (31) da Diretiva de 2019, respeitam, por exemplo a informação: ambiental; sobre o tráfego; de satélite; meteorológica e gerada por sensores. Estas informações podem ter utilizações variadas quer no plano público, quer na vertente privada. Assim, informações meteorológicas atualizadas podem ter um valor significativo em áreas como a agricultura, mas podem igualmente ser decisivas em componentes públicas como as referentes à proteção civil.

No que tange à mobilidade, informações atualizadas sobre matéria de tráfego podem ser decisivas para a criação de políticas públicas na área dos transportes com repercussão, em especial, nas áreas metropolitanas.

O Considerando distingue entre a disponibilização imediata de dados ou após a sua alteração por via de uma interface de programação de aplicações (IPA), mais frequentemente designada pelo acrónimo saxónico API (*application programming interface*). O Considerando (32) ocupa-se de uma qualificação de "IPA" simples e tecnicamente descritiva: "(…) é um conjunto de funções, procedimentos, definições e protocolos que permite a comunicação máquina-máquina e o intercâmbio contínuo de dados."

O artigo 19-A da LADA, prevê, no seu n.º 1, transpondo o artigo 5.º, números 5 e 6, da Diretiva de 2019, que os órgãos e entidades da Administração Pública disponibilizam dados dinâmicos para reutilização imediatamente após a respetiva recolha, através de IPA[12] adequado e sempre que se justifique, sob a forma de descarregamento em bloco. O n.º 2 admite limites à disponibilização imediata.

O n.º 3 determina que os dados abertos devam ser disponibilizados em catálogos de IPAs no portal dados.gov[13]. A responsabilidade pelo portal compete à

[12] Cumpre sublinhar que, nos termos da Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro, sobre a "Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o respetivo Plano de Ação Transversal para a legislatura", na Linha Estratégica III relativa a "arquiteturas de referência" existe o objetivo, indicado para 2022, de disponibilizar na Plataforma de Interoperabilidade da AP (iAP) um catálogo de IPAs.

[13] Sobre a sua caracterização, ver: https://dados.gov.pt/pt/docs/about_dadosgov/. O portal tem como função: "Além de funcionar como um serviço partilhado de alojamento e publicação de dados, que pode ser utilizado por qualquer organismo público, funciona também como um portal indexador de conteúdos alojados noutros portais/catálogos de dados abertos, sejam setoriais (ex. Saúde, Justiça, Ambiente) ou locais (ex. Municípios)."

Agência da Modernização Administrativa (AMA)[14]. As características do citado portal estão enunciadas no artigo 27.º, n.º 5 da LADA:

> "O portal dados.gov constitui-se como o catálogo central de dados abertos em Portugal, tendo como função agregar, referenciar, publicar e alojar dados abertos de diferentes organismos e setores da Administração Pública central, regional e local, funcionando também como um portal indexador de conteúdos alojados noutros portais ou catálogos de dados abertos, setoriais ou descentralizados (…)"

Os desenvolvimentos no acesso e reutilização de dados abertos – através do portal dados.gov - devem ser fundamento para o desenvolvimento de políticas públicas; basear-se num portal tecnologicamente evoluído e fomentar que as entidades públicas partilhem cada vez mais informação[15] [16]. No âmbito da União Europeia (UE) pode verificar-se, também, acesso ao Portal de Dados Abertos[17].

Apesar do conteúdo do artigo 19-A da LADA importa sublinhar que os conceitos de dados dinâmicos e dados abertos não se confundem. Os dados dinâmicos são uma categoria de dados abertos, tendo estes um alcance mais vasto[18].

---

[14] Pode consultar-se documentação contemporânea da Diretiva de 2016 aprovada pela AMA: https://www.ama.gov.pt/documents/24077/24804/guia_dados_abertos_ama.pdfN e https://www.ama.gov.pt/documents/24077/24804/guia_introdu__o_dados_abertos_ama.pdf/ .

[15] Nuno Xavier e Gabriel Osório de Barros, "Em análise dados abertos em Portugal", Gabinete de Estratégia e Estudos, data 21-11-2022, disponível em: https://www.gee.gov.pt/pt/estudos-e-seminarios/artigos-category/32493-em-analise-dados-abertos-em-portugal?highlight=WyJkYWRvcyIsImFiZXJ0b3MiLCJkYWRvcyBhYmVydG9zIl0= , p. 10.

[16] No Considerando (11) da Diretiva de 2019 afirma-se que: "A evolução para uma sociedade baseada em dados, caso sejam utilizados dados provenientes de diferentes domínios e atividades, influencia a vida de todos os cidadãos da União, permitindo-lhes, nomeadamente, obter novos meios de acesso e aquisição de conhecimento."

[17] Disponível em: https://www.europeandataportal.eu/pt/using-data/use-cases .

[18] No articulado da Diretiva de 2019 não se encontra definição de dados abertos, ao contrário do que consta no Considerando (16) que, de uma forma pouco exata, os caracteriza como: "dados em formato aberto que idealmente podem ser utilizados, reutilizados e partilhados de forma livre por qualquer pessoa e para qualquer finalidade. As políticas de livre acesso aos dados, que incentivam a ampla disponibilização e a reutilização das informações do setor público para fins privados ou comerciais, com poucas ou nenhumas restrições legais, técnicas ou financeiras, e que promovem a circulação das informações, não só para os agentes económicos mas fundamentalmente para o público em geral (…)".

1.2.2.1. Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia (RLFD).

Faremos uma análise sobre a relação entre o RLFD e o RGPD, especialmente no que respeita ao "conjunto de dados compostos por dados pessoais e não pessoais" (artigo 1.º, n.º 2 do RLFD) e referiremos as principais causas que levaram à aprovação do RLFD. Para além do instrumento normativo, será considerada a Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados (COM (2019) 250, de 29.05.2019).

Na base do RLFD está a evolução da economia baseada nos dados – e respetivas "cadeias de valor"[19] - atendendo a uma dimensão cada vez mais digital, que tem como uma das consequências o desenvolvimento da "reutilização"[20].

Para garantir a fluidez da economia digital, o RLFD cria "segurança jurídica para que as empresas possam escolher onde pretendem tratar os seus dados na UE, aumenta a confiança nos serviços de tratamento de dados e contraria as práticas de vinculação a um prestador de serviços."[21]

Como já referimos, uma das matérias importantes a tratar na análise do RLFD consiste na distinção entre dados não pessoais e dados pessoais. Deve, no entanto, reconhecer-se as vantagens dos fluxos de dados independentemente da sua

[19] Considerando (2): "As cadeias de valor de dados assentam em diferentes atividades relacionadas com os dados: criação e recolha de dados; agregação e organização de dados; tratamento de dados; análise, comercialização e distribuição de dados; utilização e reutilização de dados. O funcionamento eficaz e eficiente do tratamento de dados constitui um alicerce fundamental em todas as cadeias de valor de dados.".

[20] Considerando (1): "(…) O setor das tecnologias da informação e das comunicações deixou de ser um setor específico, passando a ser a base de todos os sistemas económicos e de todas as sociedades modernas e inovadoras. Os dados eletrónicos são um elemento central desses sistemas e podem gerar muito valor quando analisados ou combinados com serviços e produtos. Por outro lado, o rápido desenvolvimento da economia dos dados e das tecnologias emergentes, como a inteligência artificial, os produtos e serviços ligados à internet das coisas, os sistemas autónomos e a 5G, suscitam novos problemas jurídicos em torno das questões do acesso aos dados, da reutilização dos dados, da responsabilidade, da ética e da solidariedade."

[21] (COM (2019) 250), p. 2.

Para garantia da concorrência e da segurança dos dados especialmente no plano transfronteiriço, importa referir o extenso tratamento que o RLFD concede à portabilidade. Introdutoriamente, ver Considerando (29).

natureza, para a liberdade de particulares e empresas – no "grande mercado da UE" – integrados numa economia digital de mercado único[22].

1.2.2.1.1. O RLFD distingue entre dados pessoais, mantendo a definição prevista no artigo 4.º, n.º 1 do RGPD (artigo 3.º, n.º 1)[23] , dados não pessoais – ou seja, informação que não contenha dados pessoais[24] – e a conjuntos de dados compostos por dados pessoais e não pessoais (artigo 2.º, n.º 2). O RLFD refere ainda, os conjuntos de dados compostos por dados pessoais e não pessoais indissociavelmente ligados (artigo 2.º, n.º 2).

A aplicação do RLFD verifica-se quanto a dados não pessoais, valendo o RGPD no que tange a dados pessoais, particularmente, os constantes de conjuntos de dados compostos. O RLFD sublinha essa solução no caso de dados anonimizados –

---

[22] "(…) os dados podem circular livremente entre os Estados-Membros, permitindo aos utilizadores de serviços de tratamento de dados utilizar os dados recolhidos em diferentes mercados da UE para melhorar a sua produtividade e competitividade. Os utilizadores podem, assim, tirar pleno partido das economias de escala proporcionadas pelo grande mercado da UE, melhorando a sua competitividade a nível mundial e aumentando a interconectividade da economia europeia dos dados". Ibidem.

De acordo com o Considerando (10): "Nos termos do Regulamento (UE) 2016/679, os Estados-Membros não podem restringir nem proibir a livre circulação de dados pessoais no interior da União por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. O presente regulamento estabelece o mesmo princípio de livre circulação no interior da União relativamente aos dados não pessoais, com exceção dos casos em que se justifique uma restrição ou uma proibição por motivos de segurança pública. O Regulamento (UE) 2016/679 e o presente regulamento estabelecem um conjunto coerente de regras que preveem a livre circulação de diferentes tipos de dados. Por outro lado, o presente regulamento não impõe a obrigação de armazenar separadamente os diferentes tipos de dados.".

[23] "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular."

Também, Considerando (8) do RLFD.

[24] Nos termos do artigo 2.º, n.º 1 do RLFD:

"O presente regulamento aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais na União:

a) Prestado como um serviço a utilizadores residentes ou estabelecidos na União, independentemente de o prestador de serviços estar ou não estabelecido na União; ou

b) Realizado por uma pessoa singular ou coletiva com residência ou estabelecimento na União para as suas necessidades próprias."

considerados como dados não pessoais – se tornarem dados que permitam a identificação do titular por evolução tecnológica[25].

Não se encontra definição para a relação de "indissociavelmente ligação" entre dados pessoais e dados não pessoais. A solução proposta pelas Orientações da Comissão consiste em considerar que, nestas situações, a "separação dos dois tipos é impossível ou é considerada economicamente ineficiente ou tecnicamente inviável pelo responsável pelo tratamento"[26].

A notar que a definição de "tratamento", constante do artigo 3.º, n.º 2 do RLFD, tem uma proximidade relevante relativamente ao "tratamento de dados pessoais" (artigo 4.º, n.º 2 do RGPD), sendo, contudo, aplicável a dados não pessoais e a "conjuntos de dados". A aplicação do conceito respeita às diversas operações que podem ser desenvolvidas com dados, independentemente da sua natureza.

Acompanhando as Orientações da Comissão, deve distinguir-se entre os dados não pessoais que podem ser classificados segundo a sua origem entre "desde o início", tratando-se aqui de informações insuscetíveis de revestir uma natureza pessoal[27] e "posteriormente anonimizados"[28]. As Orientações sublinham que é frequente que um conjunto de dados seja composto por dados pessoais e não pessoais[29].

Do ponto de vista da relação entre proteção de dados pessoais e regime aplicável a dados não pessoais o tema mais complexo consiste nas formas de proteção de dados anonimizados que, na sequência de "evolução tecnológica" se tornam "identificados ou identificáveis".

---

[25] Artigo 2.º, n.º 2 do RLFD. Exemplificando casos de dados não pessoais e da sua utilidade económica e experimental, veja-se o Considerando (9): "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais. (…)".

[26] (COM (2019) 250), pp. 10/11.

[27] "Dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais." p. 6.

[28] Ibidem.

[29] É avançada a designação de "conjunto misto de dados" (COM (2019) 250), p. 4.

Assim, pensamos que, nos termos do RGPD, quando exista um tratamento de dados anonimizados – dados não pessoais – mas que perante a evolução tecnológica podem ser revertidos para dados pessoais permitindo a identificação dos respetivos titulares o artigo 35.º números 1 e 3, alínea a)[30].

Esta interpretação significa admitir que o RGPD, particularmente quanto às regras de *compliance* e segurança, é aplicável não apenas a dados pessoais existentes, mas a operações tecnológicas que possam vir a construir "novos" ou "de novo" dados pessoais, após a quebra da anonimização[31].

De acordo com o Grupo de Trabalho do artigo 29.º[32], apesar de não se fazer menção à transformação de dados não pessoais em dados pessoais, sustenta-se que o desenvolvimento tecnológico pode: "(…) envolver novas formas de recolha e utilização de dados, possivelmente com elevado risco para os direitos e as liberdades dos indivíduos. Na verdade, as consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma avaliação de impacto de proteção de dados [AIPD] ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da «Internet das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD."[33]
Para assegurar que são cumpridas as regras do RGPD, podem ser invocados, por exemplo, a necessidade de cumprir as regras de proteção de dados desde a

---

[30] Considerando (84); "A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco.".

[31] Para além do artigo 35.º, importa analisar os Considerandos (89) e (91). De acordo com o primeiro: "(…) nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento.".

[32] "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679." WP 248 rev.01, adotadas em 4 de abril de 2017. Revistas e adotadas pela última vez em 4 de outubro de 2017.

[33] Idem, p. 12

conceção e por defeito (artigo 25.º), a prossecução das normas de segurança do tratamento de dados pessoais (artigo 32.º) e a aprovação de procedimento de certificação (artigo 42.º)[34] .

1.2.2.2. A Diretiva de 2019 prevê a reutilização[35] de dados de empresas públicas[36] , embora com algumas limitações (artigo 1.º, n.º 1, alínea b) e artigo 3.º, n.º 2)[37] , superando o regime da Diretiva de 2003[38] .

---

[34] Manuel David Masseno, "Na Borda: Dados Pessoais e Não Pessoais nos dois Regulamentos da União Europeia" in *Disciplinarum Scientia*. Série: Sociais Aplicadas, Santa Maria, v. 16, n. 1, pp. 47-48. Disponível em : https://periodicos.ufn.edu.br/index.php/disciplinarumSA/article/view/3095.

[35] A definição prevista no artigo 2.º, n.º 11, identifica, essencialmente, as fontes da reutilização: "(…) a utilização por pessoas singulares ou coletivas de documentos na posse de: a) Organismos do setor público, para fins comerciais ou não comerciais que não correspondam ao objetivo inicial da missão de serviço público para o qual os documentos foram produzidos, excetuando o intercâmbio de documentos entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público; ou b) Empresas públicas, para fins comerciais ou não comerciais que não correspondam ao objetivo inicial de prestação de serviços de interesse geral para os quais os documentos foram produzidos, excetuando o intercâmbio de documentos entre empresas públicas e organismos do setor público exclusivamente no desempenho das funções públicas dos organismos do setor público".

[36] Com definição prevista no artigo 2.º, n.º 3: "qualquer empresa ativa nos domínios estabelecidos no artigo 1.º, n.º 1, alínea b), em relação ao qual os organismos do setor público podem exercer, direta ou indiretamente, uma influência dominante, por motivos de direito de propriedade, participação financeira ou regras que lhe sejam aplicáveis. Presume-se a existência de influência dominante dos organismos do setor público sempre que estes organismos, de forma direta ou indireta:

a) Detenham a maioria do capital subscrito da empresa;

b) Disponham da maioria dos votos correspondentes às ações emitidas pela empresa;

c) Possam designar mais de metade dos membros do órgão administrativo, de direção ou de supervisão da empresa".

[37] O Considerando (26) transmite a natureza dos dados a colher nas empresas públicas: "A presente diretiva não contém qualquer obrigação geral de autorizar a reutilização de documentos produzidos por empresas públicas. A decisão de autorizar ou não a reutilização deverá caber às empresas públicas em causa, salvo disposição em contrário da presente diretiva, do direito nacional ou da União.".

[38] Considerando (24): "(…) a Diretiva 2003/98/CE aplica-se apenas a documentos na posse de organismos do setor público, excluindo as empresas públicas do seu âmbito de aplicação. Tal conduz a uma fraca disponibilidade, para efeitos de reutilização, de documentos produzidos no âmbito da prestação de serviços de interesse geral em diversos domínios, nomeadamente no setor dos serviços de utilidade pública. Além disso, reduz consideravelmente o potencial para a criação de serviços transfronteiriços baseados em documentos na posse de empresas públicas que prestam serviços de interesse geral."

De acordo com o artigo 1.º, n.º 2, alínea b), a Diretiva não é aplicável a dados de empresas públicas:

i) produzidos fora do âmbito da prestação de serviços de interesse geral, tal como definidos na lei ou em outras normas vinculativas do Estado-Membro;

ii) relacionados com as atividades diretamente expostas à concorrência e, por conseguinte, nos termos do artigo 34.º da Diretiva 2014/25/UE[39] , não sujeitas a regras de adjudicação de contratos.

Deve notar-se, porém, que, em conformidade com o Considerando (19) se apela a que os Estados-Membros permitam a reutilização de dados constantes de "(…) documentos na posse de empresas públicas relacionados com atividades que tenham sido consideradas, nos termos do artigo 34.º da Diretiva 2014/25/UE do Parlamento Europeu e do Conselho, diretamente expostas à concorrência."

Trata-se de ir além dos requisitos mínimos da Diretiva. No Direito português, de acordo com o artigo 20.º, alínea e) da LADA os documentos na posse de empresas públicas quando relacionados com atividades diretamente expostas à concorrência não podem ser objeto de reutilização[40].

1.2.2.3. A Diretiva de 2019, no seu artigo 12.º, estabelece uma regra de inexistência de acordos de exclusividade, para efeitos de reutilização de documentos (n.º 1).

No entanto, admite-se que podem verificar-se situações em que a prossecução do interesse público justifique acordos desta natureza, que devem ser revistos de três em três anos (n.º 2).

Para assegurar garantias de transparência, sempre que haja medidas que previsivelmente permitam uma limitação da disponibilidade para reutilização de documentos por parte de entidades que não sejam o terceiro que participa no acordo, a sua publicação deve efetuar-se em linha. Os efeitos da disponibilidade dos dados destinados à reutilização devem ser objeto de exame periódico, devendo, em qualquer caso, ser revistos de três em três anos (n.º 4).

---

[39] Diretiva 2014/25/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014 relativa aos contratos públicos celebrados pelas entidades que operam nos setores da água, da energia, dos transportes e dos serviços postais e que revoga a Diretiva 2004/17/CE.

[40] Sobre reutilização na LADA ver Jorge Pação, "A reutilização da informação administrativa" in "O Acesso à informação administrativa", Tiago Fidalgo Freitas e Pedro Delgado Alves (org.), ICDP/ICJP, Almedina, 2021, pp. 341 e seguintes.

1.2.2.4. O Regulamento de execução 2023/138 da Comissão de 21 de dezembro de 2022[41], que estabelece uma lista de conjuntos específicos de dados de elevado valor e as disposições relativas à respetiva publicação e reutilização, tem na base o artigo 14.º da Diretiva de 2019 e o seu anexo I, que respeita a informações: a) geoespaciais; b) observação da Terra e do ambiente; c) meteorológicas; d) estatísticas; e) empresas e propriedade de empresas e f) mobilidade (n.º 1)[42].

Para garantir a reutilização de uma forma eficaz neste âmbito temático, o artigo 14.º, n.º 2 determina a disponibilização gratuita destes dados legíveis por máquina; acessíveis através de IPA; ou fornecidos sob a forma de descarregamento em bloco.

Esta disposição não se aplica a empresas públicas, se a disponibilização conduzisse a uma distorção da concorrência nos mercados relevantes (n.º 3), a bibliotecas (n.º 4) e quando os organismos públicos sejam obrigados a cobrir os seus custos e não se encontrem isentos dessa função (n.º 5).

A publicação e reutilização dos conjuntos de dados de elevado valor são compatíveis com a emissão de licenças-tipo abertas digitais (n.º 1)[43] . Com este regime pretende-se que a lista de conjuntos de dados de elevado valor e com "maior

[41] O Regulamento encontra-se em vigor, apesar de ainda não produzir efeitos (artigo 6.º).

[42] Deve notar-se que o Regulamento de execução faz menção expressa à da Diretiva 2007/2/CE relativa a dados de categorias geoespacial, meteorológica e de observação da Terra e do ambiente e à Diretiva 2005/44/CE relativa a dados de mobilidade (artigo 2.º, números 2 e 3).

[43] Importa verificar o Considerando (12) do Regulamento de execução: "A Diretiva (UE) 2019/1024 tem como objetivo promover a utilização de licenças públicas normalizadas disponíveis em linha para a reutilização de informações do setor público. As Orientações da Comissão sobre as licenças-tipo recomendadas, os conjuntos de dados e a cobrança de encargos pela reutilização de documentos «Comunicação da Comissão: Orientações sobre as licenças-tipo recomendadas, os conjuntos de dados e a cobrança de encargos pela reutilização de documentos (2014/C 240/01) in JO C 240 de 24.7.2014, p. 1» identificam as licenças «Creative Commons» (CC) como um exemplo de licenças públicas normalizadas recomendadas. As licenças CC são desenvolvidas por uma organização sem fins lucrativos e tornaram-se uma das principais soluções de licenciamento para informações do setor público, resultados de investigação e material do domínio cultural em todo o mundo. Por conseguinte, é necessário que o presente regulamento de execução remeta para a versão mais recente do conjunto de licenças CC, a saber, CC 4.0. Uma licença equivalente ao conjunto de licenças CC pode prever disposições adicionais, como a obrigação de o reutilizador incluir atualizações fornecidas pelo detentor dos dados e de especificar quando os dados foram atualizados pela última vez, desde que não restrinjam as possibilidades de reutilização dos dados.".

potencial socioeconómico sejam disponibilizados para reutilização com um mínimo de restrições legais e técnicas e de forma gratuita."[44]

Em sede de proteção de dados pessoais, o Regulamento de execução não contém referências no articulado, dedicando-lhe, porém, o Considerando (8). Aí se refere que a disponibilização de conjuntos de dados de elevado valor para reutilização que implique o tratamento de dados pessoais deve ser realizado em conformidade com o RGPD. A notar que não existe, contudo, menções às fontes de legitimidade previstas no artigo 6.º do RGPD. Assim, a legislação europeia não assegura a necessidade do consentimento do titular dos dados para a realização destes tratamentos, abrindo a possibilidade para, por exemplo, fundamentos de legitimidade baseados na legislação ou no interesse público.

Relativamente às metodologias a utilizar – associadas a medidas de segurança – menciona-se que: "Os Estados-Membros devem utilizar métodos e técnicas adequadas (como a generalização, a agregação, a supressão, a anonimização, a privacidade diferencial ou a aleatorização), disponibilizando assim a maior quantidade possível de dados para reutilização."

De acordo com o Considerando (7) do Regulamento de execução, o seu âmbito de aplicação não inclui os dados na posse de empresas públicas.

1.2.3. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Uma estratégia europeia para os dados (COM (2020) 66 final, Bruxelas, 19 .2.2020)[45] .

A definição da estratégia a que alude a Comunicação de 2020 baseia-se na exploração máxima de uma economia assente em dados, conduzindo a UE a modelos de desenvolvimento e liderança que permitam o progresso científico económico e social fundado no conhecimento proveniente de informação, especialmente de caráter público, já existente no mercado único: "o objetivo é criar um espaço único europeu de dados – um verdadeiro mercado único de dados,

[44] Considerando (2) do Regulamento de execução de 2023.

Com idêntico propósito, o Considerando (3) alude aos princípios FAIR: "a disponibilização de conjuntos de dados de elevado valor em condições ideais permite reforçar as políticas de livre acesso aos dados nos Estados-Membros, com base nos princípios de facilidade de localização, acessibilidade, interoperabilidade e reutilização (princípios FAIR)".

[45] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0066.

aberto a dados de todo o mundo – em que os dados pessoais e não pessoais, incluindo dados comerciais sensíveis, estejam seguros e as empresas tenham fácil acesso (…)"[46]

Neste contexto, a UE deve "melhorar as suas estruturas de governação para manuseamento de dados e de aumentar os repositórios de dados de qualidade disponíveis para utilização e reutilização."[47]

A Comunicação ressalta que a economia assente em dados permite uma "réplica praticamente a custo zero"[48] ao mesmo tempo que favorece a utilização por várias pessoas e entidades do mesmo bem.

Os propósitos assim definidos carecem de legislação adequada que regule, nomeadamente: o regime relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento 2016/679); o livre fluxo de dados não pessoais na União Europeia (Regulamento 2018/1807); os dados abertos, como temos observado na Diretiva 2019/1024 de 20 de junho e no Regulamento de execução 2023/138 da Comissão; a governação europeia de dados (Regulamento 2022/868), os serviços digitais (Regulamento 2022/2065) e a matéria da cibersegurança (Regulamento 2019/88).

Na relação com matéria de proteção de dados, a Comunicação refere a necessidade utilizar as melhores praticas no que respeita à segurança da informação como é o caso, por exemplo, da pseudonimização.[49]

Relativamente ao controlo e acesso por parte dos titulares de dados sobre informação a si respeitante, a Comunicação enfatiza o direito à portabilidade de dados pessoais (artigo 20.º do RGPD) nos "espaços de dados pessoais", assim se garantindo um controlo mais eficaz por parte do titular dos dados pessoais relativamente à informação gerada automaticamente.[50]

---

[46] COM (2020) 66 final, p. 4.

[47] Idem, p. 1.

[48] Idem, p. 4.

[49] Idem, p. 16.

[50] Idem, p. 20.

A Comunicação estabelece, também, o direito à portabilidade em referência feita a "intermediários neutros", numa alusão à proposta que veio a ser aprovada com o Regulamento 2022/868. Ibidem.

De forma mais detalhada, a Comunicação apela à relação entre a utilização e a reutilização dos dados de saúde para fins de evolução científica, desde que os titulares dos dados tenham direito a aceder e controlar os seus dados e de solicitar a sua portabilidade.[51]

Estabelecendo a relação entre a utilização e reutilização de dados pessoais e as fontes de legitimidade previstas no RGPD, a Comissão faz notar que: "os titulares dos dados precisam de estar seguros de que, após terem dado consentimento para que os seus dados sejam partilhados, os sistemas de saúde os utilizam de forma ética e garantem que o consentimento pode ser retirado a qualquer momento"[52].

Esta Comunicação frisa a necessidade de recolher informação pública em regime de dados abertos para treinar sistemas de inteligência artificial, que permita o "reconhecimento de padrões e do estabelecimento de novas correlações para técnicas de previsão mais sofisticadas conducentes a melhores decisões". [53] [54]

2. O Regulamento 2022/868[55], dos instrumentos em vigor, é o último a tratar, com densidade, a partilha e reutilização de dados por entidades públicas. É aplicável desde 24 de setembro de 2023 (artigo 38.º). O Regulamento de 2022 não prejudica a aplicação de outros instrumentos jurídicos que rejam "(…) matéria de acesso e

[51] Idem, p. 29.

[52] Ibidem.

[53] Idem, p. 3.

[54] A "vertente experimental" acompanha, em diversos passos a Comunicação: "Uma vez que é difícil compreender plenamente todos os elementos desta transição para uma economia ágil dos dados, a Comissão abstém-se deliberadamente de adotar regulamentação *ex ante* excessivamente pormenorizada e prescritiva, preferindo uma abordagem flexível da governação que favoreça a experimentação." Idem, p. 12.

Ver: Patrícia Carneiro, "Regulamento Geral sobre a Proteção de Dados e o mercado de dados – Mercado de dados 1.0 e a licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados, por via do consentimento do titular dos dados – uma imposição de base legal?" in "Anuário de Proteção de Dados", 2023, Coordenação Francisco Pereira Coutinho e Graça Canto Moniz, Universidade Nova de Lisboa. Faculdade de Direito. CEDIS, p. 156.

[55] Para uma apreciação crítica à proposta deste Regulamento, ver: "EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: https://edpb.europa.eu/our-work-tools/our documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european en.

utilização dos dados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, nem de cooperação internacional nesse contexto."[56]

O Regulamento não prejudica a aplicação do direito da concorrência (artigo 1.º, n.º 4)[57], não afetando também atividades relacionadas com a segurança pública, a defesa e a segurança nacional (artigo 1.º, n.º 5)[58]. O âmbito de aplicação do Regulamento, de acordo com o artigo 1.º, n.º 1, respeita ao seguinte:

(i) Determinação das condições para a reutilização de determinadas categorias de dados detidos por organismos do setor público;

(ii) Definição de um regime de notificação e supervisão para a prestação de serviços de intermediação de dados;

(iii) Determinação de um regime para o registo voluntário das entidades que recolhem e tratam dados disponibilizados para fins altruístas;

(iv) Estabelecer um regime para a criação de um Comité Europeu da Inovação de Dados.

(v)

2.1. No que respeita a novas normas sobre a reutilização[59], o artigo 3.º, n.º 1 do Regulamento prevê que este é aplicável a informações sobre[60]:

---

[56] Considerando (3). Também, artigo 1.º, n.º 2.

[57] Considerando (13): "Os organismos do setor público deverão respeitar o direito da concorrência ao estabelecerem os princípios de reutilização dos dados que detêm, evitando celebrar acordos que possam ter por objetivo ou efeito a criação de direitos exclusivos de reutilização de certos dados.".

[58] Ver: Considerando (3).

[59] Para efeitos deste Regulamento, reutilização está definido como "a utilização, por pessoas singulares ou coletivas, de dados detidos por organismos do setor público, realizada para fins comerciais ou não comerciais que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos, excetuando o intercâmbio de dados entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público (artigo 2.º, n.º 2).".

[60] "(…) A Diretiva (UE) 2019/1024 e o direito setorial da União garantem que os organismos do setor público tornem um maior número dos dados que produzem facilmente disponível para utilização e reutilização. No entanto, determinadas categorias de dados, como os dados comerciais confidenciais, os dados que estão sujeitos a confidencialidade estatística e os dados protegidos por direitos de propriedade intelectual de terceiros, incluindo segredos comerciais e dados pessoais, que se encontram em bases de dados públicas, muitas vezes não são disponibilizados, nem sequer para atividades de investigação ou de inovação de interesse público, apesar dessa disponibilidade ser possível nos termos do direito da União aplicável, em particular do Regulamento (UE) 2016/679 e das Diretivas 2002/58/CE e (UE) 2016/680. Devido à sensibilidade desses dados, a sua disponibilização exige o respeito prévio de certos requisitos processuais técnicos e jurídicos, principalmente para garantir o respeito

(i) Confidencialidade comercial, nomeadamente segredos comerciais, profissionais e empresariais;

(ii) Confidencialidade estatística;

(iii) Proteção dos direitos de propriedade intelectual de terceiros; ou Proteção dos dados pessoais, na medida em que os dados em causa não sejam abrangidos pelo âmbito de aplicação da Diretiva (UE) 2019/1024.

No que respeita aos casos de confidencialidade comercial, nomeadamente segredos comerciais, profissionais e empresariais, importa analisar o Considerando (10)[61], bem como o artigo 5.º, n.º 5:

> "A menos que o direito nacional preveja salvaguardas específicas sobre as obrigações de confidencialidade aplicáveis relacionadas com a reutilização de dados referidos no artigo 3.º, n.º 1, o organismo do setor público subordina a utilização dos dados fornecidos nos termos do n.º 3 do presente artigo ao cumprimento, por parte do reutilizador, de uma obrigação de confidencialidade que proíba a divulgação de qualquer informação que comprometa os direitos e interesses de terceiros e que o reutilizador possa ter adquirido apesar das salvaguardas instituídas. Os reutilizadores ficam proibidos de reidentificar qualquer titular dos dados a quem os dados digam respeito e devem tomar medidas técnicas e operacionais para prevenir a reidentificação e para notificar ao organismo do setor público qualquer violação de dados que resulte na reidentificação dos titulares dos dados em causa. Em caso de reutilização não autorizada de dados não pessoais, o reutilizador informa, sem demora, se for caso disso com a assistência do organismo do setor público, as pessoas coletivas cujos direitos e interesses possam ser afetados."

---

dos direitos de terceiros sobre os dados em questão ou limitar o impacto negativo nos direitos fundamentais, no princípio da não discriminação e na proteção de dados.".

[61] "As categorias de dados detidos por organismos do setor público cuja reutilização deverá ser regida pelo presente regulamento não são abrangidas pelo âmbito de aplicação da Diretiva (UE) 2019/1024, que exclui os dados que não são acessíveis por motivos de confidencialidade comercial ou estatística e os dados incluídos em obras ou noutro material protegido relativamente aos quais terceiros têm direitos de propriedade intelectual. Os dados comerciais confidenciais incluem os dados protegidos por segredos comerciais, o saber-fazer protegido e quaisquer outras informações cuja divulgação indevida possa ter um impacto na posição de mercado ou na saúde financeira da empresa. O presente regulamento deverá aplicar-se aos dados pessoais que não são abrangidos pelo âmbito de aplicação da Diretiva (UE) 2019/1024 na medida em que o regime de acesso exclui ou restringe o acesso a esses dados por razões de proteção de dados, privacidade e integridade da pessoa em causa, nomeadamente em conformidade com as regras em matéria de proteção de dados. A reutilização de dados que possam conter segredos comerciais deverá ter lugar sem prejuízo do disposto na Diretiva (UE) 2016/943, que estabelece o quadro para a aquisição, utilização ou divulgação legais de segredos comerciais.".

A aplicação do Regulamento às categorias de dados previstas no artigo 3.º, n.º 1 deve ser, assim, organizada:

(i) A concessão ou a recusa de acesso à reutilização de dados depende da comunicação pública a efetuar por organismos públicos que identificam pontos de identificação únicos[62] (artigo 8.º), assistidos pelos organismos competentes a que se refere o artigo 7.º, n.º 1;

(ii) "(…) O ponto de informação único é competente para receber os pedidos de informação ou os pedidos de reutilização das categorias de dados referidas no artigo 3.º, n.º 1, e transmite-os, sempre que possível e adequado por meios automatizados, aos organismos do setor público competentes (…)" (artigo 8.º, n.º 2);

(iii) O acesso e reutilização remotos dos dados devem realizar-se num ambiente de tratamento seguro disponibilizado ou controlado pelo organismo do setor público (artigo 5.º, n.º 2, alínea b))[63];

(iv) Sempre que os pedidos de reutilização puserem em causa a legislação sobre proteção de dados, particularmente o RGPD, os organismos públicos devem garantir que os "requisitos para a realização de uma avaliação de impacto em matéria de proteção de dados e a consulta da autoridade de controlo, nos termos dos artigos 35.º e 36.º do RGPD e os riscos para os direitos e interesses dos titulares dos dados tenham sido considerados mínimos, poderá ser permitida a reutilização dos dados

[62] Considerando (26): "(…) O ponto de informação único deverá dispor de uma lista de recursos com todos os recursos de dados disponíveis, incluindo, se for caso disso, os recursos de dados disponíveis nos pontos de informação setoriais, regionais ou locais, com informações relevantes que descrevam os dados disponíveis (…)."

[63] "«Ambiente de tratamento seguro» (artigo 2.º, n.º 20), o ambiente físico ou virtual e os meios organizacionais destinados a assegurar o cumprimento do direito da União, tal como o Regulamento (UE) 2016/679, em especial no que respeita aos direitos dos titulares dos dados, os direitos de propriedade intelectual, a confidencialidade comercial e estatística, a integridade e a acessibilidade, bem como o cumprimento do direito nacional aplicável e permitir à entidade que fornece o ambiente de tratamento seguro determinar e supervisionar todas as ações de tratamento de dados, incluindo visualização, o armazenamento, o descarregamento e a exportação de dados, bem como o cálculo de dados derivados através de algoritmos computacionais.".

nas instalações ou de forma remota num ambiente de tratamento seguro."[64]

2.2. De acordo com o artigo 2.º, n.º11 o Regulamento estabelece a definição de «Serviço de intermediação de dados»: "um serviço que visa estabelecer relações comerciais para efeitos de partilha de dados[65] entre um número indeterminado de titulares dos dados e detentores dos dados[66], por um lado, e utilizadores de dados[67], por outro, através de meios técnicos, jurídicos ou outros, inclusive para o exercício dos direitos dos titulares dos dados em relação aos dados pessoais, excluindo, pelo menos, o seguinte:

a) Serviços que obtêm dados junto dos detentores dos dados e agregam, enriquecem ou transformam os dados obtidos com o objetivo de lhes acrescentar um valor substancial e licenciam a utilização dos dados resultantes aos utilizadores de dados, sem estabelecer uma relação comercial entre os detentores dos dados e os utilizadores dos dados;

b) Serviços centrados na intermediação de conteúdos protegidos por direitos de autor;

c) Serviços exclusivamente utilizados por um único detentor dos dados para permitir a utilização dos dados detidos por esse detentor dos dados, ou utilizados por várias pessoas coletivas no seio de um grupo fechado, inclusive no âmbito de relações com fornecedores ou clientes ou colaborações contratualmente estabelecidas, em especial os que tenham como principal

---

[64] Considerando (15).

[65] Artigo 2.º, n.º 10: "«Partilha de dados», o fornecimento de dados, por um titular dos dados ou um detentor dos dados, a um utilizador de dados para fins da utilização conjunta ou individual dos dados em causa, com base em acordos voluntários ou no direito da União ou nacional, diretamente ou através de um intermediário, por exemplo, ao abrigo de licenças abertas ou comerciais sujeitas a uma taxa ou gratuitas.".

[66] Artigo 2.º, n.º 8: "«Detentor dos dados», uma pessoa coletiva, incluindo organismos do setor público e organizações internacionais, ou uma pessoa singular que não seja o titular dos dados no que diz respeito aos dados específicos em causa, que, em conformidade com o direito da União ou o direito nacional aplicáveis, tem o direito de conceder acesso a determinados dados pessoais ou dados não pessoais ou de os partilhar.".

[67] Artigo 2.º, n.º 9: "«Utilizador dos dados», uma pessoa singular ou coletiva que tem acesso legal a determinados dados pessoais ou não pessoais e que tem direito, inclusive ao abrigo do RGPD no que respeita aos dados pessoais, a utilizá-los para fins comerciais ou não comerciais."

objetivo assegurar funcionalidades de objetos e dispositivos ligados à Internet das coisas;

d) Serviços de partilha de dados oferecidos por organismos do setor público que não visam estabelecer relações comerciais.

Os "serviços de intermediação de dados" encontram-se explicados no Considerando (33). De modo a garantir que não existe utilização indevida ou afastada do princípio da finalidade, "é necessário que os prestadores de serviços de intermediação de dados atuem apenas como intermediários nas transações e não utilizem os dados trocados para qualquer outro fim"[68].

O Regulamento exige, também, uma separação entre o serviço de intermediação de dados e quaisquer outros serviços prestados, a fim de evitar conflitos de interesses. Assim, o serviço de intermediação de dados deverá ser prestado através de uma pessoa coletiva distinta das outras atividades desse prestador de serviços de intermediação de dados[69].

De acordo com o artigo 12.º, sublinhamos que:

(i) Os serviços de intermediação de dados podem incluir a oferta, aos detentores dos dados ou aos titulares dos dados, de instrumentos e serviços específicos adicionais que visem especificamente facilitar o intercâmbio de dados, tais como o armazenamento temporário, a curadoria, a conversão, a anonimização e a pseudonimização; os instrumentos e serviços em causa só podem ser utilizados mediante pedido ou aprovação expressos do detentor dos dados ou do titular dos dados, e os instrumentos de terceiros disponibilizados nesse contexto não podem utilizar os dados para outros fins (alínea e));

(ii) O prestador de serviços de intermediação de dados deve dispor de procedimentos para prevenir práticas fraudulentas ou abusivas de partes que procurem ter acesso através do seu serviço de intermediação de dados (alínea g));

(iii) O prestador de serviços de intermediação de dados deve tomar as medidas adequadas para assegurar a interoperabilidade com outros serviços de intermediação de dados, nomeadamente através de

[68] Considerando (33).

[69] Ibidem.

normas abertas de uso corrente no setor em que os prestadores de serviços de intermediação de dados operam (alínea i));

(iv) O prestador de serviços de intermediação de dados deve tomar as medidas necessárias para garantir um nível de segurança adequado do armazenamento, do tratamento e da transmissão de dados não pessoais, devendo ainda garantir o mais elevado nível de segurança possível do armazenamento e da transmissão de informações sensíveis do ponto de vista da concorrência (alínea l));

(v) O prestador de serviços de intermediação de dados que oferece serviços a titulares dos dados deve agir no melhor interesse destes ao facilitar o exercício dos seus direitos, em especial informando-os e, se for caso disso, aconselhando-os de forma concisa, transparente, inteligível e facilmente acessível sobre as utilizações previstas dos dados por parte dos utilizadores dos dados e sobre as condições gerais associadas a essas utilizações, antes de os titulares dos dados darem o seu consentimento (alínea m));

(vi) Caso um prestador de serviços de intermediação de dados faculte instrumentos para obter o consentimento dos titulares dos dados ou a autorização para o tratamento dos dados disponibilizados pelos detentores dos dados, deve, se for caso disso, especificar a jurisdição de país terceiro em que a utilização dos dados se destina a ser efetuada e facultar aos titulares dos dados instrumentos para dar e retirar o consentimento, e aos detentores dos dados instrumentos para dar e retirar a autorização para o tratamento de dados (alínea n)).

Entendemos que as referências episódicas ao consentimento feitas no Regulamento de 2022, não podem justificar que todos os processos de reutilização o tenham como fundamento de licitude. O Regulamento prevê a necessidade de cumprimento do RGPD, que passa pela determinação de um fundamento de legitimidade (essencialmente artigo 6.º do RGPD), não impondo o consentimento como fundamento único[70].

[70] Veja-se a crítica de Patrícia Carneiro: "Não é claro se o legislador, no Regulamento de Governação de Dados, pretendia estipular o consentimento como fundamento de licitude para o tratamento de dados pessoais no contexto do modelo de governação que institui. E, ainda que tivesse sido, tal sempre teria de ser analisado do ponto de vista do princípio da licitude estipulado na al. a) do n.º 1 do art. 5.º do RGPD. Desde logo, a respeito da compatibilização daquela imposição legal com o preceituado nos n.ºs 3 e 4 do art.º 6.º do

2.3. O artigo 2.º, n.º 16 prevê a definição de «Altruísmo de dados»: "a partilha voluntária de dados, com base no consentimento dos titulares dos dados para o tratamento dos respetivos dados pessoais ou na autorização, por parte de outros detentores dos dados, da utilização dos seus dados não pessoais, sem que esses titulares ou detentores procurem ou recebam uma gratificação que vá além de uma compensação pelos custos em que incorrem ao disponibilizarem os seus dados, para fins de interesse geral, previstos no direito nacional, se aplicável, tais como os cuidados de saúde[71], a luta contra as alterações climáticas, a melhoria da mobilidade, a facilitação do desenvolvimento, produção e divulgação de estatísticas oficiais, a melhoria da prestação dos serviços públicos, a elaboração de políticas públicas ou a investigação científica de interesse geral."[72]

O artigo 16.º prevê que os Estados-Membros podem dispor de mecanismos organizacionais ou técnicos, ou ambos, para facilitar o altruísmo de dados.

A criação de registos públicos de organizações de altruísmo de dados reconhecidas (artigo 17.º) é atualizada regularmente (n.º 1). O artigo 18.º prevê os elementos que devem constar de organizações de altruísmo.

3. Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828: introdução.

RGPD. (…) criticamos a leviandade com que o legislador desconsiderou o RGPD no Regulamento de Governação de Dados, o que era ainda mais evidente no texto da sua proposta.", pp: 177-178.

[71] Na área da saúde ver as considerações de Tiago Branco da Costa, "O Altruismo (Económico?) de dados : Breves Considerações sobre o Espaço Europeu de dados de saúde e a proteção de dados pessoais" in "Liber Amicorum Benedita Mc Crorie", Volume II, Universidade do Minho, in: https://doi.org/10.21814/uminho.ed.105.30 , p.627.

[72] Deve notar-se que: "As organizações de altruísmo de dados reguladas pelo presente regulamento não deverão ser consideradas prestadores de serviços de intermediação de dados, desde que esses serviços não estabeleçam uma relação comercial entre os potenciais utilizadores de dados, por um lado, e os titulares dos dados e os detentores dos dados que disponibilizam os dados por fins altruístas, por outro. Não deverão ser considerados serviços de intermediação de dados na aceção do presente regulamento outros serviços que não visem estabelecer relações comerciais, como os repositórios destinados a permitir a reutilização de dados de investigação científica em conformidade com os princípios do acesso aberto."

O citado Regulamento já se encontra em vigor, mas produzirá efeitos apenas a partir de 12 de setembro de 2025 (artigo 50.º)[73]. O seu conteúdo afasta-se do Regulamento de 2019 e do Regulamento de 2022, limitando a reutilização de dados, em detrimento dos mecanismos aí previstos[74]. Quanto ao conteúdo do Regulamento de 2023, revela o Considerando (5):

> "O presente regulamento garante que os utilizadores de um produto conectado ou serviço conexo[75] na União podem aceder, em tempo útil, aos dados gerados pela utilização desse produto ou serviço conexo, e que podem utilizar esses dados, nomeadamente partilhando-os com terceiros da sua escolha.

[73] Outras regras relativas à aplicabilidade do Regulamento constam, também, do artigo 50.º: "A obrigação decorrente do artigo 3.º, n.º 1, é aplicável aos produtos conectados e serviços com eles relacionados colocados no mercado após 12 de setembro de 2026.

O capítulo III é aplicável às obrigações de disponibilização de dados nos termos de disposições do direito da União ou da legislação nacional adotada em conformidade com o direito da União que entrem em vigor após 12 de setembro de 2025.

O capítulo IV é aplicável aos contratos celebrados após 12 de setembro de 2025.

O capítulo IV é aplicável a partir de 12 de setembro de 2027 aos contratos celebrados em 12 de setembro de 2025, ou antes dessa data, desde que:

a) Sejam de duração indeterminada; ou

b) Expirem pelo menos 10 anos a contar de 11 de janeiro de 2024.".

[74] Considerando (70): "O objetivo da obrigação de fornecer os dados consiste em assegurar que os organismos do setor público, a Comissão, o Banco Central Europeu ou os órgãos da União dispõem dos conhecimentos necessários para responder, prevenir ou recuperar de emergências públicas ou para manter a capacidade de desempenhar funções específicas expressamente previstas por lei. Os dados obtidos por essas entidades poderão ser comercialmente sensíveis. Por conseguinte, nem o Regulamento (UE) 2022/868 nem a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho deverão ser aplicáveis aos dados disponibilizados nos termos do presente regulamento, nem estes deverão ser considerados como dados abertos disponíveis para reutilização por terceiros. Todavia, isso não deverá afetar a aplicabilidade da Diretiva (UE) 2019/1024 à reutilização de estatísticas oficiais para cuja elaboração tenham sido utilizados dados obtidos nos termos do presente regulamento, desde que a reutilização não inclua os dados subjacentes.".

[75] Artigo 2.º, n.º 6 "«Serviço conexo», um serviço digital, que não seja um serviço de comunicações eletrónicas, incluindo software, conectado ao produto no momento da aquisição ou locação de tal modo que a sua ausência impediria que o produto conectado desempenhasse uma ou mais das suas funções, ou conectado posteriormente ao produto pelo fabricante ou por terceiros, a fim de aumentar, atualizar ou adaptar as funções do produto conectado."

De acordo com o Considerando (6): "A geração de dados é o resultado das ações de, pelo menos, dois intervenientes, nomeadamente o projetista ou o fabricante de um produto conectado, que, em muitos casos, pode ser também um prestador de serviços conexos, e o utilizador do produto conectado ou serviço conexo. Suscita questões de equidade na economia digital, uma vez que os dados registados por produtos conectados ou serviços conexos constituem um contributo importante para os serviços pós-venda, complementares e outros (…)."

> Impõe aos detentores dos dados a obrigação de disponibilizarem dados aos utilizadores e a terceiros escolhidos pelo utilizador em determinadas circunstâncias.
> Garante também que os detentores dos dados disponibilizam os dados aos destinatários dos dados na União ao abrigo de cláusulas e condições equitativas, razoáveis e não discriminatórias e de forma transparente. As regras do direito privado são fundamentais no regime global da partilha de dados.
> Por conseguinte, o presente regulamento adapta as regras do direito contratual e impede a exploração dos desequilíbrios contratuais que dificultam o acesso equitativo aos dados e a sua utilização. O presente regulamento garante também que, em caso de necessidade excecional, os detentores dos dados disponibilizam aos organismos do setor público, à Comissão, ao Banco Central Europeu ou aos órgãos da União os dados necessários para o desempenho de uma função específica de interesse público. Além disso, visa facilitar a mudança entre serviços de tratamento de dados e reforçar a interoperabilidade dos dados e dos mecanismos e serviços de partilha de dados na União. O presente regulamento não deverá ser interpretado como reconhecendo ou como conferindo aos detentores dos dados qualquer novo direito de utilizar os dados gerados pela utilização de um produto conectado ou serviço conexo."

A proteção de dados pessoais no Regulamento de 2023 é mencionada de forma acentuada no Considerando (7):

> "(…) O presente regulamento complementa e não prejudica o direito da União em matéria de proteção de dados pessoais e privacidade, nomeadamente os Regulamentos (UE) 2016/679 e (UE) 2018/1725 e a Diretiva 2002/58/CE. Nenhuma disposição do presente regulamento deverá ser aplicada ou interpretada de forma a diminuir ou limitar o direito à proteção dos dados pessoais ou o direito à privacidade e à confidencialidade das comunicações. Qualquer tratamento de dados pessoais nos termos do presente regulamento deverá cumprir o direito da União em matéria de proteção de dados, incluindo o requisito de que haja um fundamento jurídico válido para o tratamento nos termos do artigo 6.º do Regulamento (UE) 2016/679 (…)."

Referências:

Jorge Pação, "A reutilização da informação administrativa" in "O Acesso à informação administrativa", Tiago Fidalgo Freitas e Pedro Delgado Alves (org.), ICDP/ICJP, Almedina, 2021;

Manuel David Masseno, "Na Borda: Dados Pessoais e Não Pessoais nos dois Regulamentos da União Europeia" in *Disciplinarum Scientia*. Série: Sociais Aplicadas, Santa Maria, v. 16, n. 1, pp. 47-48. Disponível em: https://periodicos.ufn.edu.br/index.php/disciplinarumSA/article/view/3095;

Nuno Xavier e Gabriel Osório de Barros, "Em análise dados abertos em Portugal", Gabinete de Estratégia e Estudos, data 21-11-2022, disponível em: https://www.gee.gov.pt/pt/estudos-e-seminarios/artigos-category/32493-em-analise-dados-abertos-em-portugal?highlight=WyJkYWRvcyIsImFiZXJ0b3MiLCJkYWRvcyBhYmVydG9zIl0;

Patrícia Carneiro, "Regulamento Geral sobre a Proteção de Dados e o mercado de dados – Mercado de dados 1.0 e a licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados, por via do consentimento do titular dos dados – uma imposição de base legal?" in "Anuário de Proteção de Dados", 2023, Coordenação Francisco Pereira Coutinho e Graça Canto Moniz, Universidade Nova de Lisboa. Faculdade de Direito. CEDIS;

Tiago Branco da Costa, "O Altruismo (Económico?) de dados: Breves Considerações sobre o Espaço Europeu de dados de saúde e a proteção de dados pessoais" in "Liber Amicorum Benedita Mc Crorie", Volume II, Universidade do Minho, in: https://doi.org/10.21814/uminho.ed.105.30;

Parecer n.º 3/99, sobre preservação de dados de tráfico de ISPs para finalidades de *law enforcement*: Grupo de Trabalho do artigo 29.º, 5085/99/EN/FINAL WP 25, 7 de setembro de 1999;

Parecer n.º 5/2001, sobre o Relatório Especial do Provedor de Justiça Europeu ao Parlamento Europeu na sequência do projeto de recomendação à Comissão Europeia relativo à reclamação 713/98/IJH: Grupo de Trabalho do artigo 29.º, 5003/00/EN/Final WP 44, 17 de maio de 2001;

Parecer n.º 7/2003, sobre a reutilização da informação do sector público e proteção dos dados pessoais - Estabelecer um equilíbrio: Grupo de Trabalho do artigo 29.º, 10936/03/PT WP 83, 12 de dezembro de 2003;

Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados (COM (2019) 250, de 29.05.2019);

EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: https://edpb.europa.eu/our-work-tools/ourdocuments/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en;

Diretiva do Conselho 90/313/CEE, de 7 de junho de 1990, relativa à liberdade de acesso à informação em matéria de ambiente;

Diretiva 2003/98/CE do Parlamento Europeu e do Conselho de 17 de novembro de 2003 relativa à reutilização de informações do sector público;

Diretiva 2013/37/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público;

Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público;

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);

Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia;

Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados);

Regulamento de execução 2023/138 da Comissão de 21 de dezembro de 2022, que estabelece uma lista de conjuntos específicos de dados de elevado valor e as disposições relativas à respetiva publicação e reutilização;

Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828;

Lei n.º 26/2016, de 22 de agosto, Lei de Acesso aos Documentos Administrativos – (LADA);

Lei n.º 68/2021, de 26 de agosto, Aprova os princípios gerais em matéria de dados abertos e transpõe para a ordem jurídica interna a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informação do setor público, alterando a Lei n.º 26/2016, de 22 de agosto;

Declaração de Retificação n.º 31/2021, de 20 de setembro, publicado no DRE (Série I), de 26 de agosto de 2021;

Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro, sobre a "Estratégia para a Transformação Digital da Administração Pública 2021-2026.

Da publicação na Internet das atas de reuniões de órgãos colegiais autárquicos: uma leitura (crítica) da orientação de 18 de abril de 2023 da CNPD

Isabel Celeste M. Fonseca*

Joel A. Alves**

Resumo

Tendo como mote a Orientação de 18 de abril de 2023 da CNPD, relativa à publicação na Internet das atas de reuniões de órgãos colegiais, o presente artigo visa refletir sobre as restrições a que poderá ser sujeito o acesso a atas de órgãos colegiais administrativos - em especial, órgãos autárquicos - das quais constem dados pessoais. Para tanto, começar-se-á por apresentar o regime-geral traçado pela LADA, quanto ao acesso a documentos administrativos (§1). De seguida, procurar-se-á analisar como tal regime tem sido concretamente aplicado pela CADA, nos casos em que esteja em causa o acesso a atas de órgãos colegiais da Administração Pública (§2). Por fim, colocar-se-á a tónica na supramencionada orientação de 18 de abril de 2023 da CNPD, efetuando uma leitura crítica sobre o posicionamento jurídico nela sufragado (§3). Terminar-se-á com algumas notas conclusivas, procurando, essencialmente, dar resposta a duas interrogações fundamentais:

* Professora Associada da Escola de Direito da Universidade do Minho. Investigadora Principal no âmbito do projeto «Smart Cities and Law, E.Governance and Rights: Contributing to the definition and implementation of a Global Strategy for Smart Cities», ref. NORTE-01-0145-FEDER-000063.

** Assistente Convidado na Escola de Direito da Universidade do Minho. Doutorando em Ciências Jurídicas, na especialidade de Ciências Jurídicas Públicas, na Escola de Direito da Universidade do Minho. A colaboração no presente escrito foi efetuada com o apoio financeiro da Fundação para a Ciência e Tecnologia, ao abrigo da Bolsa de Investigação para Doutoramento melhor identificada pela referência 2022.13673.BD.

poderá a publicação de atas de reuniões de órgãos colegiais locais na Internet considerar-se juridicamente admissível? Em caso afirmativo, sob que condições?

Palavras-chave: atas; documentos administrativos; documentos nominativos; dados pessoais; transparência; informação reservada.

From the publication on the Internet of the minutes of meetings of local collegiate bodies: a (critical) reading of the CNPD guidance of April 18, 2023

Abstract

Taking as its motto the Guidance of April 18, 2023 of the CNPD, regarding the publication on the Internet of minutes of meetings of collegial bodies, this article aims to reflect on the restrictions to which access to minutes of administrative collegial bodies may be subject - in especially, local authorities - which contain personal data. To this end, we will begin by presenting the general regime outlined by LADA, regarding access to administrative documents (§1). Next, we will attempt to analyze how this regime has been concretely applied by CADA, in cases where access to minutes of collegial Public Administration bodies is at stake (§2). Finally, the emphasis will be placed on the aforementioned guidance of April 18, 2023 from the CNPD, carrying out a critical reading of the legal position supported therein (§3). It will end with some conclusive notes, essentially seeking to answer two fundamental questions: could the publication of minutes of meetings of local collegiate bodies on the Internet be considered legally permissible? If so, under what conditions?

Keywords: minutes; administrative documents; nominative documents; personal data; transparency; reserved information.

Enquadramento

Na prossecução das atribuições que lhe são cometidas, enquanto autoridade de controlo nacional para efeitos do Regulamento Geral sobre a Proteção de Dados[76] e da Lei n.º 58/2019, de 8 de agosto[77], veio a Comissão Nacional de Proteção de Dados (=CNPD) recentemente aprovar cinco orientações dotadas de especial relevância para o setor público[78].

De entre estas, conta-se, designadamente, a Orientação de 18 de abril de 2023, relativa à publicação na Internet das atas de reuniões de órgãos colegiais. Matéria que, não sendo nova[79], continuara, nas palavras da referida entidade administrativa, a revelar-se "frequentemente objeto de consulta e de pedido de esclarecimentos"[80]. O que, na sua ótica, justificara levar a um público mais vasto o que viera sendo o seu entendimento sobre a mesma[81].

Tendo isso como mote, o presente artigo visa refletir sobre as restrições a que poderá ser sujeito o acesso a atas de órgãos colegiais administrativos - em especial, órgãos autárquicos - das quais constem dados pessoais. Para tanto, começar-se-á por apresentar o regime-geral traçado pela Lei de Acesso aos Documentos Administrativos[82], quanto ao acesso a documentos administrativos (1). De seguida,

---

[76] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados (de ora em diante, abreviadamente designado por RGPD).

[77] Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.

[78] Cfr. CNPD, "Novas orientações da CNPD", 5 de maio de 2023, disponível em https://www.cnpd.pt/comunicacao-publica/noticias/novas-orientacoes-da-cnpd/ [Consultado a 11 de maio de 2023].

[79] Sobre o tema, vd. Acórdão da Relação do Porto de 07/11/2019 RP201911071606/17.4T8PVZ.P1, disponível em www.dgsi.pt, consultado em 23 de janeiro de 2020 (IV – A quebra do segredo profissional e o acesso da ATA a dados sobre factos da vida íntima dos cidadãos não depende de permissão da Lei da Protecção de Dados Pessoais. V – A Lei da Protecção de Dados Pessoais não impede a comunicação dos dados a terceiros desde que nessa comunicação exista um objectivo legítimo que seja susceptível de justificar uma ingerência na vida privada, o que cabe às ordens jurídicas nacionais definir.)

[80] Idem.

[81] Idem.

[82] Lei n.º 26/2016, de 22 de agosto, que prova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE,

procurar-se-á analisar como tal regime tem sido concretamente aplicado pela Comissão de Acesso aos Documentos Administrativos (=CADA), nos casos em que esteja em causa o acesso a atas de órgãos colegiais da Administração Pública (2). Por fim, colocar-se-á a tónica na supramencionada orientação de 18 de abril de 2023 da CNPD, efetuando uma leitura crítica sobre o posicionamento jurídico nela sufragado (3). Terminar-se-á com algumas notas conclusivas, procurando, essencialmente, dar resposta a duas interrogações fundamentais: poderá a publicação de atas de reuniões de órgãos colegiais locais na Internet considerar-se juridicamente admissível? Em caso afirmativo, sob que condições? (4).

1. O regime-geral da LADA

1.1. A regra do livre acesso

Dito isto, importa recordar que as atas das reuniões de órgãos autárquicos configuram documentos administrativos, na aceção do artigo 3.º, n.º 1, alínea a), da LADA[83]. Donde, salvo legislação específica em contrário, a sua disponibilização deva necessariamente realizar-se de acordo com as condições gerais de acesso, consagradas nesse mesmo diploma[84].

Nesta senda, estabelece o artigo 5.º, n.º 1, da LADA, enquanto regime-regra, que "todos, sem necessidade de enunciar qualquer interesse, têm direito de acesso aos documentos administrativos". O que significa que, por princípio, qualquer documento "diretamente produzido ou recolhido no exercício normal de funções administrativas"[85] - i.e. que haja sido elaborado ou se encontre na posse "de

do Parlamento Europeu e do Conselho, de 17 de novembro (de ora em diante, abreviadamente designada por LADA).

[83] Nesse sentido, cfr., entre outros, CADA, Parecer n.º 214/2023, Processo n.º 5/2023, 19 de julho de 2023, p. 2; CADA, Parecer n.º 111/2023, Processo n.º 10009/2022, 19 de abril de 2023, p. 2; CADA, Parecer n.º 365/2021, Processo n.º 445/2021, 16 de dezembro de 2021, p. 1.

[84] Para mais desenvolvimentos, cfr. Pratas, Sérgio, A (nova) Lei de Acesso aos Documentos Administrativos, Almedina, Coimbra, 2018, p. 66.

[85] Seguimos aqui a noção de "documento administrativo" proposta por Caupers, João, "Sobre o conceito de documento administrativo", in Cadernos de Justiça Administrativa, n.º 75, p. 9. Definição essa que, aliás, tem sido reiteradamente acolhida pela jurisprudência dos tribunais administrativos superiores portugueses. Nesse sentido, veja-se, entre outros arestos, (i) o Acórdão do STA (1.ª Secção de Contencioso Administrativo), de 10 de março de 2022, Processo n.º 02063/21.6BELSB; (ii) o Acórdão do STA (1.ª Secção de Contencioso Administrativo), de 10 de setembro de 2014, Processo n.º 0410/14; e (iii) o Acórdão do TCA-N

entidades públicas ou privadas, por efeito da sua atuação, ainda que circunstancial, no exercício de prerrogativas de autoridade ou segundo um regime de direito administrativo"[86] - deve presumir-se "de acesso livre e irrestrito"[87].

A justificação para tal é simples. Afinal, conquanto não goze de positivação expressa na Constituição da República Portuguesa ou no Código do Procedimento Administrativo[88], é hoje pacífico que o *princípio da transparência da atividade administrativa* se apresenta como um elemento "consubstancial a toda a ordem jurídica democrática"[89], "constituindo mesmo condição indispensável para o exercício da cidadania e da participação na vida pública e para a responsabilização (*accountability*) e o controlo externo dos poderes públicos"[90].

Dito de outro modo: não sofre hoje controvérsia que "só num sistema administrativo inspirado pela transparência se pode realizar, na sociedade, uma efetiva atividade propositiva, participativa e de controlo, bem como o valor da cidadania administrativa"[91]. Daí a comum asserção de que uma *Administração democrática* não pode deixar de afirmar-se como uma *Administração transparente*[92]; uma verdadeira "casa de vidro"[93], que, muito embora não prescindindo de "algumas

(1.ª Secção de Contencioso Administrativo), de 20 de dezembro de 2019, Processo n.º 01414/19.8BEPRT.

[86] Cfr. ALMEIDA, Mário Aroso de / CADILHA, Carlos Alberto Fernandes, *Comentário ao Código de Processo nos Tribunais Administrativos*, 4.ª edição, Almedina, Coimbra, 2017, p. 857.

[87] Sublinhando que é este o princípio-geral aplicável em matéria de acesso a documentos administrativos, por força do disposto no artigo 5.º, n.º 1, da LADA, cfr. CADA, Parecer n.º 357/2021, Processo n.º 752/2021, 16 de dezembro de 2021, p. 5.

[88] Alertando para tal facto, cfr. FARINHO, Domingos Soares, "Princípio da administração aberta: a evolução do direito positivo português", *in O Acesso à Informação Administrativa* (org. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, p. 12; FERNANDES, Débora Melo, "O princípio da transparência administrativa: mito ou realidade?", *Revista da Ordem dos Advogados*, Ano 75, Jan-Jul 2015, pp. 427-429.

[89] Nesse sentido, cfr. Acórdão do Tribunal Constitucional (1.ª secção), de 30 de junho de 1992, Processo n.º 34/90.

[90] Cfr. FERNANDES, Débora Melo, "O princípio da transparência administrativa: mito ou realidade?", *Revista da Ordem dos Advogados*, Ano 75, Jan-Jul 2015, p. 427.

[91] Cfr. GONÇALVES, Pedro Costa, *Manual de Direito Administrativo,* vol. 1, Almedina, Coimbra, 2019, p.485.

[92] Nesse sentido, cfr. MORÓN, Miguel Sánchez, *Derecho Administrativo: parte general*, 16.ª edição, Tecnos, Madrid, p. 81.

[93] Cfr. ANTUNES, Luís Filipe Colaço, "Mito e realidade da transparência administrativa", in Boletim da Faculdade de Direito da Universidade de Coimbra, 1993, p. 16.

janelas protegidas ou fechadas"[94], promove uma cultura de tendencial abertura e revelação, permitindo aos cidadãos saberem o que ela sabe[95], para, assim, averiguarem da *legalidade* e *mérito* da sua atuação[96].

Daqui decorre que, quaisquer órgãos e entidades cobertos pelo âmbito de aplicação subjetivo da LADA - como sejam, para o que aqui importa, os órgãos das autarquias locais[97] - "têm, quando solicitados, o dever de facultar a sua documentação administrativa"[98].

Mais: independentemente dos pedidos que lhes sejam dirigidos, impõe-se a tais órgãos e entidades que coloquem em prática "uma política ativa de informação aberta e transparente que facilite e promova o controlo difuso da sua ação pelos cidadãos"[99] - assim o determina o artigo 2.º, n.º 2, da LADA, onde se lê que "a informação pública relevante para garantir a transparência da atividade administrativa, designadamente a relacionada com o funcionamento e controlo da atividade pública" deve ser "divulgada ativamente, de forma periódica e atualizada, pelos respetivos órgãos e entidades". Obrigação que o artigo 10.º, n.º 1, do mesmo diploma complementa e concretiza, estabelecendo que, para o efeito, tais órgãos e entidades devem, nomeadamente, publicitar nos seus sítios na Internet, de forma periódica e atualizada, no mínimo semestralmente, "os documentos administrativos (...) que entendam disponibilizar livremente para acesso e reutilização", bem como toda "a informação cujo conhecimento seja relevante para garantir a transparência da atividade relacionada com o seu funcionamento".

---

[94] Idem, ibidem.

[95] Cfr. AMORIM, João Pacheco / OLIVEIRA, Mário Esteves de / GONÇALVES, Pedro Costa, *Código do Procedimento Administrativo - Comentado*, Almedina, Coimbra, 2010, p. 342.

[96] Em sentido próximo, sustentando que "a promoção da transparência funciona como fator de controlo da própria vinculação da Administração à legalidade e ao mérito", cfr. FARINHO, Domingos Soares, "Princípio da administração aberta: a evolução do direito positivo português", *in O Acesso à Informação Administrativa* (org. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, p. 18.

[97] Cfr. artigo 4.º, n.º 1, alínea e), da LADA.

[98] Cfr. Acórdão do STA (1.ª Secção do Contencioso Administrativo), de 6 de janeiro de 2010, Processo n.º 0965/09.

[99] Cfr. GONÇALVES, Pedro Costa, *Manual de Direito Administrativo,* vol. 1, Almedina, Coimbra, 2019, p.485

1.2. As restrições aplicáveis ao acesso a documentos administrativos nominativos

Se é certo que na atividade administrativa a regra deve ser a informação e não o segredo[100], tal não significa, porém, que os órgãos e entidades anteriormente referidos não possam, face a certas circunstâncias, limitar o acesso à documentação administrativa na sua posse. É que, sendo embora um *direito fundamental de natureza análoga aos direitos, liberdades e garantias*[101], "o direito de acesso aos documentos administrativos não é um direito absoluto, pois pode colidir com outros bens ou direitos legalmente protegidos"[102]. Circunstância que pode, naturalmente, justificar a sua restrição, por forma a que seja assegurada a necessária concordância prática entre todos os valores jurídicos em confronto.

Ora, é precisamente o que se verifica quanto aos designados "documentos nominativos", isto é, documentos administrativos que contenham dados pessoais, na aceção do artigo 4.º, n.º 1, do RGPD[103]. Documentos esses que, no respeito pelo disposto no artigo 35.º da Constituição da República Portuguesa - e, em especial, pelo princípio vertido no seu n.º 4, segundo o qual "é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei" -, o legislador entendeu submeter a um regime específico de proteção.

---

[100] Nesse sentido, veja-se, entre outros, o Acórdão do STA de 20 de janeiro de 2010, Processo n.º 01110/09, bem como o Acórdão do STA (1.ª Subsecção do Contencioso Administrativo) de 30 de setembro de 2009, Processo n.º 0493/09, e o Acórdão do STA (1.ª Subsecção do Contencioso Administrativo) de 17 de janeiro de 2008, Processo n.º 0896/07.

[101] Cfr., *inter alia*, o Acórdão do STA (2.ª Subsecção do Contencioso Administrativo), de 21 de setembro de 2010, Processo n.º 0562/10, bem como o Acórdão do TCA-N (1.ª Secção do Contencioso Administrativo), de 13 de julho de 2012, e o Acórdão do TCA-S (1.ª Secção do Contencioso Administrativo), de 19 de outubro de 2017, Processo n.º 856/17.8BELRA.

[102] Cfr. Acórdão do TCA-S (1.ª Secção do Contencioso Administrativo), de 4 de novembro de 2010, Processo 06744/10. Em sentido idêntico, veja-se, ainda o Acórdão do STA (2.ª Subsecção do Contencioso Administrativo), de 8 de julho de 2009, Processo n.º 0451/09, bem como o Acórdão do TCA-N (1.ª Secção do Contencioso Administrativo), de 14 de fevereiro de 2007, Processo n.º 01180/06.7BEPRT.

[103] Cfr. artigo 3.º, n.º 1, alínea b), da LADA. Recorde-se que, nos termos do supramencionado artigo 4.º, n.º 1 do RGPD, entende-se por dados pessoais qualquer "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)". Sendo que, de acordo com o mesmo preceito, deve considerar-se "identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". Para mais desenvolvimentos, cfr., com as necessárias adaptações, Grupo de Trabalho de Proteção de Dados do Artigo 29.º, "Parecer 4/2007 sobre o conceito de dados pessoais", 20 de junho de 2007.

Assim, e em derrogação da regra-geral de livre acesso, prevista no seu artigo 5.º, n.º 1, dispõe o artigo 6.º, n.º 5, da LADA, que um terceiro só tem direito de acesso a documentos administrativos nominativos: (i) se estiver munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que quer aceder; ou (ii) se demonstrar fundamentadamente ser titular de um interesse, direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante que, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, justifique o acesso à informação.

Sem embargo, deixa o artigo 6.º, n.º 9, do mesmo diploma, ainda assim, ressalvado que, "nos pedidos de acesso a documentos nominativos que não contenham dados pessoais que revelem a origem étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, dados genéticos, biométricos ou relativos à saúde, ou dados relativos à intimidade da vida privada, à vida sexual ou à orientação sexual de uma pessoa, presume-se, na falta de outro indicado pelo requerente, que o pedido se fundamenta no direito de acesso a documentos administrativos". O que aponta para a aplicação de um regime jurídico diferenciado, consoante esteja em causa o acesso a documentos administrativos que contenham *dados pessoais de categorias especialmente protegidas* - seja nos termos do RGPD[104], seja nos termos do nosso texto constitucional[105] - ou o «mero» acesso a documentos administrativos que contenham *dados pessoais de categorias comuns*[106].

Passamos a explicar. Estando em causa documentos administrativos que contenham *dados pessoais de categorias especialmente protegidas*, será de aplicar integralmente o disposto no supramencionado artigo 6.º, n.º 5, da LADA. Pelo que, salvo a existência de autorização escrita do titular dos dados, prestada de acordo com as condições previstas nesse mesmo preceito, o acesso à documentação administrativa somente poderá ser concedido se o requerente demonstrar fundamentadamente *ser titular de um interesse, direto, pessoal, legítimo e*

[104] Cfr. artigo 9.º, n.º 1, do RGPD.

[105] Cfr. artigo 35.º, n.º 3, da Constituição da República Portuguesa.

[106] Em sentido idêntico, cfr. FABIÃO, Gonçalo de Andrade, "Restrições de acesso à informação administrativa: dados pessoais", in *O Acesso à Informação Administrativa* (coord. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, pp. 225-226.

constitucionalmente protegido suficientemente relevante que, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, justifique o acesso à informação.

Já estando em causa documentos administrativos que «apenas» contenham *dados pessoais de categorias comuns*, o artigo 6.º, n.º 5, da LADA, deve ser lido em conjugação com o artigo 6.º, n.º 9, do mesmo diploma. O que quer dizer que, para aceder à documentação pretendida, "não é exigido que o requerente apresente interesse direto, pessoal, legítimo e constitucionalmente protegido diferente do direito de acesso a documentos administrativos"[107]. Antes lhe basta fazer uso deste direito e, bem assim, demonstrar, após ponderação, no quadro do princípio da proporcionalidade, que o seu exercício justifica, *in casu*, o sacrifício do direito à proteção de dados pessoais dos demais envolvidos[108].

2. A jurisprudência da CADA

Perante isto, tem a CADA entendido que "de uma forma geral, as atas de órgãos da Administração Pública são subsumíveis à regra de livre acesso, prevista no já citado artigo 5.º, n.º 1, da LADA"[109]. Contudo, nem por isso esta entidade administrativa deixa de reconhecer que pode existir nesses documentos "informação reservada, designadamente, de natureza nominativa e irrelevante à atividade administrativa, por isso, não livremente acessível"[110].

Exemplo disso é o que sucede com os números de identificação civil e fiscal, a morada, ou os números de telefone e telemóvel de pessoas singulares[111]. Tudo isto, *dados pessoais*, na aceção do artigo 4.º, n.º 1, do RGPD. E, bem assim, "elementos cujo conhecimento, em princípio, nada acrescentaria à faculdade de controlo da atividade administrativa"[112]. O que justifica que a sua disponibilização a terceiros

[107] Idem, p. 226.

[108] Idem, ibidem.

[109] Cfr. CADA, Parecer n.º 246/2023, Processo n.º 153/2023, 19 de julho de 2023, p. 4.

[110] Cfr. CADA, Parecer n.º 214/2023, Processo n.º 5/2023, 19 de julho de 2023, p. 3.

[111] Idem, ibidem.

[112] Idem, pp. 4-5.

possa ser objeto de restrições - contrariamente a outros *dados, de natureza meramente funcional*, tais como o nome dos membros dos órgãos públicos que participaram na reunião, os quais devem ser de acesso livre, em nome dos princípios da transparência e do controlo público da atividade administrativa[113].

Não obstante, ponto é que mesmo o acesso a atas onde constem *dados pessoais de natureza não meramente funcional* não deve ser condicionado na sua totalidade. De todo. Segundo a melhor jurisprudência da CADA, a obtenção da necessária concordância prática entre o *direito de acesso aos documentos administrativos* e o *direito à proteção de dados pessoais*, numa situação jurídico-factual com esse tipo de contornos, passa por uma solução diversa - qual seja, a disponibilização da documentação em causa com o expurgo da eventual informação de carácter reservado que nela possa existir[114]. Posicionamento que, diga-se, vai em linha com o previsto no artigo 6.º, n.º 8, da LADA, onde se lê que "os documentos administrativos sujeitos a restrições de acesso são objeto de comunicação parcial sempre que seja possível expurgar a informação relativa à matéria reservada".

De resto, estranho seria se assim não fosse. Afinal, para além de documentos administrativos, as atas de órgãos colegiais da Administração Pública constituem instrumentos aos quais o nosso ordenamento jurídico atribui uma específica *função de publicidade:* "as atas das reuniões de órgãos colegiais visam, por natureza, registar e dar a conhecer a emissão das deliberações tomadas nas reuniões dos órgãos colegiais"[115]. Assim resulta, de forma cristalina, do disposto no artigo 34.º, n.º 1, do Código do Procedimento Administrativo, nos termos do qual se estabelece que "de cada reunião é lavrada ata, que contém um resumo de *tudo o que nela tenha ocorrido e seja relevante para o conhecimento e a apreciação da legalidade das deliberações tomadas*" (destaque nosso).

Por outras palavras: as atas das reuniões de órgãos colegiais administrativos - tais como os órgãos das autarquias locais - existem, nada mais nada menos, do que para *levar ao conhecimento do público* tudo o que de relevante naquelas tenha ocorrido,

---

[113] Cfr. CADA, Parecer n.º 77/2021, Processo n.º 30/2021, 24 de março de 2021, p. 4.

[114] Nesse sentido, cfr., entre outros, CADA, Parecer n.º 73/2023, Processo n.º 976/2022, 15 de março de 2023, p. 3.

[115] Cfr. CNPD, "Orientação relativa à publicação na Internet das atas das reuniões de órgãos colegiais", p. 1.

designadamente, por forma a possibilitar o *controlo da legalidade* - e, quando tal se justifique, do próprio *mérito* - das deliberações ali tomadas. Objetivo que, evidentemente, estaria condenado ao fracasso, caso estas se configurassem como *documentos de acesso restrito*.

Nestes termos, o entendimento perfilhado pela CADA parece-nos não apenas lógico como equilibrado: "as atas são, em regra documentos de acesso livre. Se eventualmente nelas existir alguma matéria reservada, deve a mesma ser expurgada nessa parte"[116] - reitera-se, *apenas e só nessa parte*, sob pena de a restrição em causa se afigurar ilegítima, traduzindo-se numa injustificada denegação do direito de acesso aos documentos administrativos.

3. A Orientação da CNPD de 18 de abril de 2023

Ocorre que, tal como a CNPD teve ocasião de advertir, no quadro da já citada orientação de 18 de abril de 2023, relativa à publicação na Internet das atas de reuniões de órgãos colegiais, a consulta das atas não se confunde com a respetiva publicação na Internet[117]. Isto porque, nas palavras da autoridade de controlo nacional, para efeitos do RGPD e da Lei n.º 58/2019, de 8 de agosto, a divulgação de documentos administrativos que contenham dados pessoais na Internet "significa a permanente disponibilização de tais dados, muito para além do espaço territorial nacional e do período de tempo necessário, ou seja, do perímetro dos interessados e do período temporal pertinentes. A que acresce a circunstância de, nesse contexto de rede aberta, os dados pessoais serem ou poderem ser objeto de reutilização por qualquer um para qualquer finalidade, inclusive ilegítima, em face da dificuldade ou mesmo impossibilidade de rastrear o seu tratamento por terceiros. Demais, o relacionamento automático com outros dados relativos à mesma pessoa, permite ou potencia a criação de perfis sobre as pessoas e de subsequente tomada de decisões (ou de outros atos) que afetem diretamente a esfera jurídica dos seus titulares"[118].

[116] Cfr. CADA, Parecer n.º 73/2023, Processo n.º 976/2022, 15 de março de 2023, p. 3.

[117] CNPD, "Orientação relativa à publicação na Internet das atas das reuniões de órgãos colegiais", p. 1.

[118] Idem, pp. 1-2.

Quer isto dizer, em suma, que a divulgação ativa de documentos administrativos nominativos na Internet comporta riscos substancialmente elevados[119], de todo incomparáveis com os que se verificam no panorama clássico em que a administração detém a informação, o particular pede o acesso e a informação é disponibilizada. Circunstância que, naturalmente, determina a sua sujeição a um regime mais restritivo - sob pena de uma excessiva e intolerável compressão de direitos fundamentais como o direito à proteção de dados pessoais, o direito ao respeito pela vida privada, ou o direito à igualdade (na vertente de não discriminação) dos titulares das informações objeto de disseminação[120].

Nesta senda, a posição da CNPD é clara: por norma, a publicação de atas de órgãos colegiais administrativos na Internet apenas se deverá considerar admissível quando estas não contenham dados pessoais[121]. Estando em causa documentos nominativos, deve a documentação em jogo ser anonimizada - isto é, expurgada de todos os dados pessoais nela constantes - previamente à sua divulgação[122]. Caso contrário "a publicação na Internet não será admissível (...) atenta a repercussão que (...) pode ter na vida das pessoas visadas e considerando que existem meios capazes de garantir ainda o princípio da transparência, sem expor de modo permanente e para além do universo de potenciais interessados nas informações"[123].

O único desvio que a CNPD admite a este princípio-regra prende-se com a divulgação de atas que contenham deliberações administrativas que se encontrem legalmente sujeitas a publicação na Internet - tal como sucede, para o que aqui releva, com as *deliberações dos órgãos colegiais locais destinadas a ter eficácia externa*[124]. Nestes casos - sublinhe-se, *apenas e só nestes casos* - a autoridade de

[119] Idem, ibidem.

[120] Idem, p. 2.

[121] Idem, p. 3.

[122] Idem, ibidem.

[123] Idem, p. 2.

[124] Assim decorre do artigo 56.º da Lei n.º 75/2013, de 12 de setembro, onde se prescreve que "[p]ara além da publicação em Diário da República quando a lei expressamente o determine, as deliberações dos órgãos das autarquias locais, bem como as decisões dos respetivos titulares destinadas a ter eficácia externa, devem ser publicadas em edital afixado nos lugares de estilo durante cinco dos 10 dias subsequentes à tomada da deliberação ou decisão, sem prejuízo do disposto em legislação especial" (n.º 1). E, bem assim, que "[o]s atos referidos no número anterior são ainda publicados no sítio da Internet, no boletim da autarquia

controlo nacional prefigura a publicação de atas com dados pessoais na Internet como possível, desde que realizada "em cumprimento dos princípios da proporcionalidade e da minimização dos dados, consubstanciados na alínea c) do n.º 1 do artigo 5.º do RGPD"[125]. O que, nas suas palavras, nomeadamente, implica que as atas a publicar sejam elaboradas "com a redução ao indispensável dos dados que integrem as categorias previstas no n.º 1 do artigo 9.º e no artigo 10.º do RGPD - por exemplo, eventuais decisões relativas a procedimentos disciplinares devem ser registadas em ata por referência ao número do processo, sem identificação do trabalhador visado"[126].

4. Conclusões

Do exposto, podem, pois, extrair-se as seguintes conclusões:

i. Estando em causa o *acesso a atas de órgãos colegiais administrativos, através de pedido formulado nos termos do artigo 12.º, n.º 1, da LADA*, deve este ser concedido:
   a. sempre que a documentação concretamente solicitada *não contenha dados pessoais*, e não se verifiquem outras restrições, previstas na LADA ou em legislação especial, que impeçam a sua disponibilização a terceiros;
   b. sempre que a documentação concretamente solicitada *apenas contenha dados pessoais de natureza funcional* (e.g. identificação de quem esteve presente na reunião a que a ata se refere, e em nome de quem esteve presente);
   c. sempre que a documentação concretamente solicitada *contenha outro tipo de dados pessoais*, na medida em que a entidade requerida proceda ao expurgo da informação de carácter reservado que nelas existas (e.g. números de identificação civil e fiscal; moradas; números

local e nos jornais regionais editados ou distribuídos na área da respetiva autarquia, nos 30 dias subsequentes à sua prática" (n.º 2).

[125] CNPD, "Orientação relativa à publicação na Internet das atas das reuniões de órgãos colegiais", p. 3.

[126] Idem, ibidem.

de telefone e telemóvel de pessoas singulares; etc.), previamente à sua disponibilização.

ii. Existindo nas atas de órgãos colegiais administrativos *deliberações legalmente sujeitas a publicação na Internet* – tal como sucede com as deliberações dos órgãos colegiais locais destinadas a ter eficácia externa - devem as deliberações em questão ser ativamente divulgadas no *website* institucional de tais entidades. O que, todavia - e contrariamente ao que a CNPD parece sugerir, na sua orientação de 18 de abril de 2023, relativa à publicação na Internet das atas de reuniões de órgãos colegiais -, não implica que as atas nas quais essas deliberações se integram tenham, elas próprias, de ser publicadas. Pelo contrário: o que se exige é a divulgação ativa das *deliberações*. Não das *atas*, na sua globalidade.

iii. Na ausência de disposição legal específica, através da qual expressamente se comine a obrigatoriedade de *publicação na Internet das atas de órgãos colegiais administrativos,* apenas se poderá considerar tal publicação como admissível caso:

   a. a documentação ativamente divulgada *não contenha dados pessoais*, ou qualquer outra informação sujeita a restrições de acesso, nos termos da LADA (e.g. segredos comerciais, industriais ou sobre a vida de uma empresa) ou de legislação especial (e.g. informação coberta pelo regime do segredo de Estado, aprovado pela Lei Orgânica n.º 2/2014, de 6 de agosto).

   b. *contendo dados pessoais* – e/ou qualquer outra informação de carácter reservado – esses elementos sejam objeto de expurgo, previamente à publicação.

De facto, no que especificamente respeita a este último ponto, o artigo 10.º, n.º 5, da LADA é claro: "a divulgação ativa da informação deve acautelar o respeito pelas restrições de acesso previstas na presente lei, devendo ter lugar a divulgação parcial sempre que seja possível expurgar a informação relativa à matéria reservada". Solução que, diga-se, encontra-se em harmonia, quer com a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público – onde se estabelece que os Estados-Membros devem incentivar os organismos do setor público e as empresas públicas a produzir e disponibilizar documentação em conformidade com o princípio

«abertos desde a conceção e por defeito»[127] -, quer com o Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022, relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) – onde, por sua vez, se determina que os organismos do setor público devem assegurar, em conformidade com o direito da União e nacional, que a natureza protegida dos dados que pretendam disponibilizar seja preservada; o que pode justificar a adoção de requisitos, tais como os de que o acesso para fins de reutilização de dados apenas deverá ser concedido se o organismo do setor público ou o organismo competente, na sequência de um pedido de reutilização, *tiver assegurado que os dados foram anonimizados, no caso dos dados pessoais, ou foram alterados, agregados ou tratados por qualquer outro método de controlo da divulgação, no caso das informações comerciais confidenciais, incluindo os segredos comerciais ou conteúdos protegidos por direitos de propriedade intelectual*[128].

Bibliografia

ALMEIDA, Mário Aroso de / CADILHA, Carlos Alberto Fernandes, *Comentário ao Código de Processo nos Tribunais Administrativos*, 4.ª edição, Almedina, Coimbra, 2017.

AMORIM, João Pacheco / OLIVEIRA, Mário Esteves de / GONÇALVES, Pedro Costa, *Código do Procedimento Administrativo - Comentado*, Almedina, Coimbra, 2010.

ANTUNES, Luís Filipe Colaço, "Mito e realidade da transparência administrativa", in Boletim da Faculdade de Direito da Universidade de Coimbra, 1993, pp. 1-55.

CAUPERS, João, "Sobre o conceito de documento administrativo", *in Cadernos de Justiça Administrativa*, n.º 75, pp. 3-10.

FABIÃO, Gonçalo de Andrade, "Restrições de acesso à informação administrativa: dados pessoais", in *O Acesso à Informação Administrativa* (coord. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, pp. 209-235.

[127] Cfr. artigo 5.º, n.º 2, da Diretiva.

[128] Cfr. artigo 5.º, n.º 3, alínea a), do Regulamento.

FARINHO, Domingos Soares, "Princípio da administração aberta: a evolução do direito positivo português", *in O Acesso à Informação Administrativa* (org. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, pp. 7-29.

FERNANDES, Débora Melo, "O princípio da transparência administrativa: mito ou realidade?", *Revista da Ordem dos Advogados*, Ano 75, Jan-Jul 2015, pp. 425-457.

GONÇALVES, Pedro Costa, *Manual de Direito Administrativo,* vol. 1, Almedina, Coimbra, 2019, p.485.

MORÓN, Miguel Sánchez, *Derecho Administrativo: parte general*, 16.ª edição, Tecnos, Madrid,

PRATAS, Sérgio, *A (nova) Lei de Acesso aos Documentos Administrativos*, Almedina, Coimbra, 2018.

Jurisprudência citada

STA (1.ª Secção de Contencioso Administrativo), Acórdão de 10 de março de 2022, Processo n.º 02063/21.6BELSB.

STA (1.ª Secção de Contencioso Administrativo), Acórdão de 10 de setembro de 2014, Processo n.º 0410/14.

STA (2.ª Subsecção do Contencioso Administrativo), Acórdão de 21 de setembro de 2010, Processo n.º 0562/10.

STA (1.ª Subsecção do Contencioso Administrativo), Acórdão de 20 de janeiro de 2010, Processo n.º 01110/09.

STA (1.ª Secção do Contencioso Administrativo), Acórdão de 6 de janeiro de 2010, Processo n.º 0965/09.

STA (1.ª Subsecção do Contencioso Administrativo), Acórdão de 30 de setembro de 2009, Processo n.º 0493/09.

STA (2.ª Subsecção do Contencioso Administrativo), Acórdão de 8 de julho de 2009, Processo n.º 0451/09.

STA (1.ª Subsecção do Contencioso Administrativo), Acórdão de 17 de janeiro de 2008, Processo n.º 0896/07.

TCA-N (1.ª Secção de Contencioso Administrativo), Acórdão de 20 de dezembro de 2019, Processo n.º 01414/19.8BEPRT.

TCA-N (1.ª Secção do Contencioso Administrativo), Acórdão de 13 de julho de 2012.

TCA-N (1.ª Secção do Contencioso Administrativo), Acórdão de 14 de fevereiro de 2007, Processo n.º 01180/06.7BEPRT.

TCA-S (Secção de Contencioso Administrativo), Acórdão de 8 de setembro de 2022, Processo n.º 399/22.8BESNT.

TCA-S (Secção de Contencioso Administrativo), Acórdão de 19 de outubro de 2017, Processo n.º 856/17.8BELRA.

TCA-S (1.ª Secção do Contencioso Administrativo), Acórdão de 4 de novembro de 2010, Processo 06744/10.

Tribunal Constitucional (1.ª secção), Acórdão de 30 de junho de 1992, Processo n.º 34/90.

Outros documentos

CADA, Parecer n.º 345/2023, Processo n.º 205/2023, 13 de setembro de 2023.
CADA, Parecer n.º 246/2023, Processo n.º 153/2023, 19 de julho de 2023.
CADA, Parecer n.º 214/2023, Processo n.º 5/2023, 19 de julho de 2023.
CADA, Parecer n.º 111/2023, Processo n.º 1009/2022, 19 de abril de 2023.
CADA, Parecer n.º 73/2023, Processo n.º 976/2022, 15 de março de 2023.
CADA, Parecer n.º 333/2022, Processo n.º 588/2022, 14 de setembro de 2022.
CADA, Parecer n.º 74/2022, Processo n.º 692/2021, 16 de março de 2022.
CADA, Parecer n.º 365/2021, Processo n.º 445/2021, 16 de dezembro de 2021.
CADA, Parecer n.º 357/2021, Processo n.º 752/2021, 16 de dezembro de 2021.

CADA, Parecer n.º 322/2021, Processo n.º 446/2021, 10 de novembro de 2021.

CADA, Parecer n.º 260/2021, Processo n.º 564/2021, 8 de setembro de 2021.

CADA, Parecer n.º 77/2021, Processo n.º 30/2021, 24 de março de 2021.

CADA, Parecer n.º 141/2020, Processo n.º 294/2020, 14 de julho de 2020

CADA, Parecer n.º 18/2021, Processo n.º 674/2020, 20 de janeiro de 2020.

CNPD, Orientação relativa à publicação na Internet das atas de reuniões de órgãos colegiais, 18 de abril de 2023.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, "Parecer 4/2007 sobre o conceito de dados pessoais", 20 de junho de 2007.

Dos ataques de *ransomware* na *Convenção de Budapeste sobre o Crime Cibernético*, um ensaio de qualificação alternativa, desde Portugal[129] – [130]

Manuel David Masseno[131]

[129] Este texto foi escrito para a Obra Coletiva *Ransomware 360°: Abordagens multidisciplinares da extorsão criptoviral*, organizada por Emerson Wendt e Guilherme Gueiros, a ser publicada no Brasil, no primeiro semestre de 2024.

[130] Por opção de princípio, apenas cito estudos de Autores portugueses, os quais têm de lidar com a vigência da *Convenção do Conselho da Europa sobre o Cibercrime* / *Convenção* [do Conselho da Europa] *sobre o Crime Cibernético*, adotada em Budapeste, a 23 de novembro de 2001, desde quando esta foi aprovada e ratificada em simultâneo com a aprovação da nova *Lei do Cibercrime*, a Lei n.º 109/2009, de 15 de setembro <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174>, e que estejam em Acesso Aberto, ainda que apenas em repositórios, pois o objetivo principal de este texto consiste em abrir novas veredas para as pesquisa dos Juristas brasileiros. Os interessados em aprofundar esta temática encontrarão aí múltiplas referências adicionais, tanto portuguesas quanto de Doutrinas estrangeiras, as quais estiveram também subjacentes à preparação de este breve estudo, além de obras mais recentes, como as de Duarte Rodrigues NUNES (2020). *Os Crimes Previstos na Lei do Cibercrime*. Coimbra: Gestlegal, e de Pedro Dias VENÂNCIO (2022). *Lições de Direito do Cibercrime. E da tutela penal de dados pessoais*. Editora d'Ideias, ainda não referenciadas pelos trabalhos indicados nas Referências bibliográficas presentes no final de este texto. Embora deva ser tido em atenção que, na sua generalidade, mesmo quando abordam a *Convenção*, os Autores enfrentam as questões imersos em um contexto legislativo, jurisprudencial e doutrinário essencialmente nacional, requerendo uma especial prudência crítica no sentido de evitar transposições intersistemáticas apressadas.

[131] Em Portugal, é Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo Investigador [*i.e.*, Pesquisador] Colaborador do CEG-UAb – Centro de Estudos Globais da Universidade Aberta e Membro Convidado do CDPC – Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, ambas de Lisboa. Desde há mais de uma década, leciona sobre matérias de Direito Penal da Informática no MESI do IPBeja, assim como no Mestrado em Direito e Informática da Escola de Direito da Universidade do Minho e, mais recentemente, também na Pós-Graduação em Direito e Tecnologia da Faculdade de Direito da Universidade Católica Portuguesa – Porto. Para contacto: <masseno@ipbeja.pt>.

Resumo

Por efeito da muito recente adesão à Convenção do Conselho da Europa sobre o Cibercrime, de 2001 (a *Convenção de Budapeste*), o Brasil terá de adequar o respetivo Direito Penal Material. Este o artigo avalia a viabilidade de enquadrar primariamente os ataques de *ransomware* no crime de "Fraude [Burla] informática", em atenção tanto aos elementos objetivos e subjetivos quanto aos bens jurídicos protegidos, os quais sempre tiveram por finalidade alargar ao máximo a criminalização de atos contra o património praticados através de meios informáticos, conforme à "Minuta do Relatório Explicativo da Convenção". São ainda objeto de estudo os concursos possíveis com outros crimes constantes da *Convenção*, como a "Violação de dados [Dano provocado nos dados]" e a "Interferência em sistema [Sabotagem informática]", com o inerente "Uso indevido de aparelhagem [Utilização indevida de dispositivos]" para a prática de ataques de *ransomware*, e ainda a "Falsificação informática" e o "Acesso ilegal [ilícito]".

Palavras-chave: Brasil, burla informática, Convenção sobre o Cibercrime, *ransomware*

From the ransomware attacks at the Budapest Convention on Cybercrime, an essay alternative qualification, from Portugal

Abstract
As a result of the very recent adherence to the Convention of the Council of Europe on Cybercrime, of 2001 (the *Budapest Convention*), Brazil will have to adequate its Substantive Criminal Law. This paper evaluates the viability of considering ransomware attacks within the scope of "Computer-related fraud", considering the acts and the intents of this offence as well as the legal stated protected interests, that was designed in order to include at most computer-related illegal transfers of property trough data or system manipulations, according to the "Explanatory Report to the Convention on Cybercrime". The possible cumulation with other crimes included in the *Convention*, such as "Data interference" and "System interference", along with the "Misuse of devices" intended to perform acts related with ransomware attacks, offenses, as well as "Computer-related forgery" and "Illegal access", are also comprised in the subject of study.

Keywords: Brazil, computer-related fraud, Convention on Cybercrime, ransomware

1. Pontos de partida

Como por confessar que a efetiva razão de ser deste meu contributo passou pela necessidade de me reposicionar relativamente ao artigo escrito com Emerson Wendt, "ainda a quente", aquando dos ataques com o *WannaCry* e as questões relativas ao seu enquadramento no âmbito do Direito Penal alcançaram uma projeção global[132].

Aliás, embora redigido em poucos dias e com objetivos assumidamente humildes, sobretudo consistentes em facultar referências sólidas às Polícias e aos Ministérios Públicos de Portugal e do Brasil na investigação e perseguição criminais de tais ações, esse artigo ficou como uma referência quase obrigatória nos estudos subsequentes sobre a matéria em língua portuguesa, com múltiplas referências em livros, artigos e trabalhos académicos.

Em síntese extrema, intentámos uma caraterização material de tais ataques, em termos dinâmicos e explorando as variações em presença, e formulámos propostas de qualificação de cada um dos correspondentes passos nos Ordenamentos penais português e brasileiro, atendendo à falta de uma tipificação específica em ambos, a qual continua a se verificar quase sete anos depois. O que fizemos recorrendo ao conjunto das previsões incriminatórias, mesmo para além dos delitos informáticos em sentido próprio. A que se seguiu uma análise sumária dos concursos, tanto reais quanto aparentes, entre os tipos identificados e analisados.

Cumpre ainda acrescentar que esta perspectiva antecipou a seguida, vários anos depois, pela *Nota de Orientação* emitida a este propósito pelo *Comité da Convenção sobre o Crime Cibernético* (Comité T-CY)[133]. Embora esta proporcione sobretudo um entendimento estático, em mosaico, enquanto a nossa o fazia dinamicamente, enquanto fluxo operativo, distinguindo as possíveis variantes nas vias de ataque de *ransomware*, como já referimos[134].

---

[132] Concretamente, M.D. MASSENO & E. WENDT (2017, *passim*).

[133] Emitida em inglês como T-CY *Guidance Note #12 Aspects of ransomware covered by the Budapest Convention* (T-CY(2022)14), aprovada a 30 de novembro de 2022, a qual também abrange as matérias de Direito Processual e de Cooperação Internacional pertinente, estando disponível neste endereço: <https://www.coe.int/en/web/cybercrime/-/ransomware-new-guidance-note-by-the-t-cy>; ainda a este propósito, aproveito o ensejo para acrescentar que Portugal tem sido eleito, e sucessivamente reeleito, para este Comité desde 2006, sendo sempre representado por Pedro Verdelho, Coordenador do Gabinete Cibercrime da Procuradoria-Geral da República <https://cibercrime.ministeriopublico.pt/>.

[134] Num sentido próximo, embora centrado nas Fontes portugueses, as quais tiveram por fundo, sucessivamente, a *Recomendação n.º R (89) 9*, de 13 de setembro de 1989, relativa à criminalidade informática, do Comité de Ministros dos Estados-Membros do Conselho da Europa e a *Convenção de Budapeste*, assim como as Diretivas relevantes da União Europeia, além de facultar uma profusão de referências documentais e doutrinárias, D.R. NUNES (2019, *passim*). A *Recomendação* do Comité de Ministros está disponível em inglês, designadamente pela Organização dos Estados Americanos: <https://www.oas.org/juridico/english/89-

Porém, cerca de um ano depois, por ocasião do *II Congresso Nacional* [brasileiro] *de Direito Digital*, organizado pela Comissão de Direito Digital da Seção de Santa Catarina da Ordem dos Advogados do Brasil, em finais de abril de 2018, a maturação resultante da continuidade do estudo da matéria conduziu-me a um novo entendimento de ordem sistemática no que se refere à qualificação dos ataques de *ransomware*, precisamente por referência à *Convenção sobre o Crime Cibernético*[135-136], a *Convenção de Budapeste*.

9&final%20Report.pdf>; enquanto as versões oficiais, em inglês e francês, assim como todas oficiosas, da podem ser consultadas na correspondente página do Conselho da Europa: <https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations>.

[135] Uma análise que tivera também por referência explícita a Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32013L0040>, M.D. MASSENO (2018a). Embora a circunstância de, ao tempo, a Decisão-quadro do Conselho, de 28 de maio de 2001, relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001F0413> ainda vigorar não tenha contribuído para um mais fácil reposicionamento da perspectiva, como porventura teria ocorrido se já tivesse saído a subsequente Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019L0713>, sobre a qual, ainda que com a tónica na Lei n.º 79/2021, de 24 de novembro, que a transpôs para o Ordenamento português <https://diariodarepublica.pt/dr/detalhe/lei/79-2021-174824631>, é de indicar o estudo de D.R. NUNES (2022). Porém, o Direito da União Europeia não constitui o objeto deste trabalho, ainda que uma argumentação assentando nos mesmos fosse até suscetível de contribuir para um melhor esclarecimento das questões que enfrentamos.

[136] Entendimento este que tenho vindo a explorar, desde várias vertentes, no âmbito da lecionação nas disciplinas de "Direito na Segurança Informática e no Cibercrime", "Cibercriminalidade" e "Cibercrime e Prova Digital", designadamente no Mestrado em Direito e Informática da Universidade do Minho, M.D. MASSENO (2023a).

Entretanto, a muito recente, ainda que tardia, adesão do Brasil à *Convenção*[137-138], com a inerente necessidade de "adotar medidas legislativas e outras providências necessárias", adequando o respectivo Direito Penal Material[139], levaram-me a alinhar algumas reflexões, sobretudo com a finalidade de contribuir para o debate que deve anteceder a criminalização de novas condutas ou a modificação do enquadramento de condutas já antes penalizadas[140].

O que não será um exercício simplesmente académico, vazio de relevância prática, sendo a *Convenção* fragmentária, de mínimos e, consequentemente, deixar uma ampla margem de conformadora para o Poder Legislativo interno de cada uma das Partes, como mostra a *Nota de Orientação* do Comité T-CY, já referida.

---

[137] Na sequência de um processo longo, formalmente desencadeado com a sinalização diplomática da sua disponibilidade para ser convidado a aderir à *Convenção*, em julho de 2019, com o convite a ser efetivado em dezembro de esse ano, embora a Presidência da República apenas tenha enviado para o Congresso a proposta de ratificação legislativa com a Mensagem nº 412, de 22 de julho de 2020, com a adesão a ser aprovada por meio do Decreto Legislativo nº 37, de 16 de dezembro de 2021, e a promulgação ocorrer através do Decreto nº 11.491, de 12 abril de 2023 <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm>. Embora do Decreto constar que "a República Federativa do Brasil firmou a Convenção sobre o Crime Cibernético, em Budapeste, em 23 de novembro de 2001", essa indicação apenas pode resultar de um *lapsus calami*, pois do texto resulta também que "Governo brasileiro [apenas] depositou, junto ao Secretário-Geral do Conselho da Europa, em 30 de novembro de 2022, o instrumento de ratificação à Convenção", não sendo um dos subscritores iniciais. Sobre estas vicissitudes, embora em termos muito sintéticos, M.D. Masseno (2023b).

[138] Sobre a *Convenção*, em termos gerais, embora sobretudo centrada nas suas previsíveis consequências para as Fontes legislativas portuguesas, temas as páginas introdutórias de P. VERDELHO (2003, *passim*), assim como e sobretudo as reflexões de F.P. CARVALHO, O. MORALES G. & M. ÁLVAREZ F. (2018, 48-54), além dos meus apontamentos atualizados, MASSENO (2023a).

[139] Como, aliás, procurei mostrar na minha muito recente Aula Aberta para a WB Educação, M.D. MASSENO (2023b).

[140] É de sublinhar que o Brasil optou por se afastar da terminologia e da estrutura frásica das Versões já publicadas em língua portuguesa, designadamente, da de natureza oficiosa do próprio Conselho da Europa <https://rm.coe.int/16802fa428>, assim como das oficiais de Portugal, constante da Resolução da Assembleia da República n.º 88/2009, em 10 de Julho de 2009 <https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/88-2009-489698>, e de Cabo Verde, conforme à Resolução [da Assembleia Nacional] n.º 116/VIII/2014, de 19 de novembro <https://kiosk.incv.cv/V/2014/11/19/1.1.70.1929/p2107>, tendo ido diretamente à versão oficial em inglês <https://rm.coe.int/1680081561>, embora sem a seguir exatamente, inclusive ao traduzir "*Convention on Cybercrime*" por "Convenção sobre o Crime Cibernético". Ora, esta "liberdade legística" poderá ter consequências, como veremos em seguida, as quais deverão ser evitadas aquando da aprovação da lei, ou leis, de adequação do Ordenamento penal brasileiro à Convenção, sobretudo tendo em vista o conteúdo e o alcance *Princípio da tipicidade penal*, previsto no inciso XXXIX do Artigo 5º da *Constituição Federal* de 1988.

2. Uma qualificação primária

Começando por recordar a caracterização dos ataques de *ransomware*, em sentido próprio, feita por mim e por E. Wendt, a qual mantenho:

"Em extrema síntese, o mesmo pode-se resumir em quatro passos, todos eles necessários para a identificação do nosso objeto:

(1) a obtenção de acesso ao sistema informático da vítima, com ou sem engano, por parte do(s) autore(s);

(2) a que se segue a inserção no referido sistema de um código, o qual encripta dados, com base em um mecanismo de chaves assimétricas, gerando adicionalmente uma identificação personalizada desse mesmo sistema;

(3) depois, tem lugar uma comunicação à vítima do ocorrido, assim como do montante exigido, para facultar/entregar a chave personalizada de desencriptação, enviando valores em criptomoedas (para não ser rastreável), e o endereço (carteira) para onde deve ser enviado, junto com a identificação personalizada do sistema em causa; e

(4) finalmente, uma vez, efetuado o pagamento, a vítima recebe uma chave personalizada de desencriptação que lhe permite recuperar os dados."[141]

Se nos abstrairmos de pré-entendimentos resultantes do *nomen juris* atribuído ao tipo, o qual teria sempre uma importância secundária, podemos identificar todos os traços caracterizadores de tais ataques no crime correspondente à "Fraude informática".

Aliás, é patente como o texto da *Convenção* contem uma noção muito ampla de "fraude", *rectius* de "objetivo fraudulento", nos dolos específicos facultativos dos tipos correspondentes ao "Acesso ilegal" (Artigo 2), "Interceptação ilícita" (Artigo 3) e "Falsificação informática" (Artigo 7), o usando para assinalar um desvalor de relativo à intenção de alguém se apropriar ilicitamente de bens alheios.

Adicionalmente, atendendo ao explicitado na "Minuta do Relatório Explicativo" apensa à *Convenção*, a qual acompanharemos de perto, enquanto contraponto aos enunciados normativos, a tipificação da "Fraude informática" foi concebida de modo a abranger um espectro amplo de práticas ilícitas contra o património, em ambiente informático:

"A revolução tecnológica veio multiplicar as possibilidades de cometer infracções de carácter económico, tais como as fraudes, das quais citamos as fraudes verificadas com os cartões de crédito. Os activos representados ou

[141] Sobre estes, inclusive identificando variantes, são de assinalar os desenvolvimentos de D.R. NUNES (2019, 61-68) e as considerações muito recentes, embora breves, de J.C. PINTO (2023).

administrados por sistemas informáticos (fundos eletrónicos, dinheiro de depósitos) tornam-se alvos de manipulações da mesma maneira que as tradicionais formas de propriedade. Estes crimes consistem principalmente na manipulação da entrada no sistema, em que são introduzidos dados incorretos, ou em manipulações em programas e outras interferências no tratamento de dados. [Consequentemente] **O objetivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento de dados, cuja intenção seja a de efectuar uma transferência indevida de propriedade** [negrito meu]"[142].

Portanto, podemos ter por assente que o preceito foi concebido e redigido cuma grande abertura, de modo a abranger as novas realidades sociais e tecnológicas suscetíveis de alcançar os resultados indesejados, embora sempre de natureza essencialmente patrimonial, o que nos permite enquadrar ações ainda desconhecidas ou inviáveis à época por razões de ordem tecnológica. Assim, da *Convenção* consta o tipo relativo à:

"Artigo 8 - **Fraude informática** [negrito meu]

Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de:

a. qualquer inserção, alteração, apagamento ou supressão de dados de computador;

b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita."[143_144]

---

[142] Assim, no Ponto 36 da *Minuta*, a qual está também acessível em língua portuguesa, embora seguindo a norma europeia anterior ao *Acordo Ortográfico* de 1990 <https://rm.coe.int/16802fa429>. Do mesmo modo e ainda mais claramente, estes objetivos constam do Ponto II.2.a do *Relatório* do Comité Europeu de Problemas Criminais do Conselho da Europa, apenso à *Recomendação n.º R (89) 9*, já referido e que teve uma importância fundamental nos trabalhos preparatórios da *Convenção*, como é assumido tanto na *Minuta de qua* quanto no *Preâmbulo* da própria *Convenção*.

[143] Esta redação segue de perto a constante do *Relatório* apenso à *Recomendação n.º R (89) 9*, de 13 de setembro de 1989, em cujos termos a "Computer related fraud" [aliás, a primeira das condutas a serem criminalizadas] consiste em: "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for oneself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property)". A *Recomendação* do Comité de Ministros, incluindo o *Relatório*, por esta recebido, estão disponíveis em inglês, designadamente pela Organização dos Estados Americanos: <https://www.oas.org/juridico/english/89-9&final%20Report.pdf>.

[144] Efetivamente, esta conceptualização corresponde ao estado dos debates a propósito de estas questões, designadamente quanto à inserção do § 263a "Computerbetrug" [Fraude informática] no *Strafgesetzbuch* (StGB) [*Código Penal*, alemão] através da "Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität" [a Segunda Lei para Combater a Criminalidade

Passando a uma análise do tipo, sempre na perspectiva dos ataques de *ransomware*, no referente ao seu elemento objetivo, temos enquanto objetos necessários e alternativos da ação ou os "dados de computador", entendidos como "qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa;" (Artigo 1 b.) ou o "sistema de computador" [o qual] designa qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de dados;" (Artigo 1 a.).

A este propósito, é necessário entender que o "programa" é abrangido pela noção de "dados de computador" e por "aparelho" deve ser considerado não apenas um esquipamento físico (*hardware*), mas também os programas de computador que permitem o respectivo funcionamento (*software*), como resulta explicitamente do texto da *Convenção*, a propósito da criminalização de atos preparatórios, ao incluir o "programa de computador" na noção de "aparelho" (Artigo 6º parágrafo 1, letra a i)[145].

Económica], de 15 de maio de 1986, a qual dispõe, quanto ao nosso objeto de estudo, que "1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.". Por sua vez, a *Recomendação* esteve na base da *Primeira Geração* de Leis europeias sobre a matéria, como ocorreu em Itália com a inclusão do art. 640 ter "Frode informática" no *Codice Penale*, pela "Legge 23 dicembre 1993 n. 547", pela qual "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto com qualsiasi modalita' su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se' o ad altri un ingiusto profitto con altrui danno, e' punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.", assim como em Portugal, aproveitando a reforma profundada do *Código Penal*, operada pelo Decreto-Lei n.º 48/95, de 15 de março, ao inserir o Art.º 221.º "Burla informática", "1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.", a propósito deste preceito, embora em termos contextualizados com a *Recomendação* e também com a posterior *Convenção*, têm interesse as reflexões de C.G. PEDRA (2019, 15-19), assim como de C. RODRIGUES (2019, 44-45), D.S. PALMA (2019, 77-82 e 84-86) e de P.L.R. MOTA (2019, 171-173).

[145] Neste ponto, é indispensável ter em atenção que, como resulta explicitamente do Ponto 22 da *Minuta*, "Foi considerado pelos autores do projeto que, ao abrigo da presente Convenção, as Partes não ficariam obrigadas a copiar textualmente, para as suas legislações nacionais, os quatro conceitos definidos no Artigo 1°, desde que tais conceitos se encontrem abrangidos nas referidas legislações de uma forma coerente com os princípios da *Convenção* e proporcionem uma estrutura equivalente para a sua implementação.". Ora, no Ponto 22, a propósito do "sistema de computador" consta que este "é um equipamento composto por *hardware* e *software* desenvolvidos para o tratamento automático de dados digitais

Por sua vez, no que se refere à caracterização do conteúdo da ação típica, temos dois elementos de natureza objetiva, em alternativa e de forma relativamente vinculada, consistentes em "qualquer inserção, alteração, apagamento ou supressão de dados de computador" ou em "qualquer interferência no funcionamento de um computador ou de um sistema de computadores", incluindo o próprio *hardware*. O que nos ataques de *ransomware* é efetivado por meio da encriptação ou cifragem de dados ou programas, o Passo 2) no procedimento descrito.

Quanto ao elemento subjetivo do tipo, temos um dolo genérico correspondente a "causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem", ao qual acresce o dolo específico que subjaz à "intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita". Correspondendo aos objetivos essenciais dos ataques, consistentes na obtenção de um pagamento por parte da vítima, a qual procura assim recuperar o controle dos dados e ou do sistema, os Passos 3) e 4).

Ainda a propósito do alcance do dolo específico indicado, apesar de uma interpretação apenas enunciativa apontar para o inverso, é indispensável acrescentar que o mesmo releva para as duas condutas típicas e não apenas em caso de "interferência no funcionamento de um computador ou de um sistema de computadores". Como nos mostra uma leitura comparativa entre as versões oficiais e vinculantes, em inglês[146] e em francês[147], assim como as outras versões em língua

---

[enquanto] a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador.".

[146] "Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

[147] "Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.".

portuguesa, a oficiosa do Conselho da Europa[148] e as correspondentes às aprovações para ratificação de Portugal e de Cabo Verde[149], as quais coincidem, *verbatim*.

Nestes termos, estamos perante um crime de dano, a ser consumado com o prejuízo patrimonial efetivo da vítima, para tal não bastando à "inserção, alteração, apagamento ou supressão de dados de computador" ou a "interferência no funcionamento de um computador ou de um sistema de computadores". Embora destas ações, em si mesmo consideradas possam também resultar danos de natureza patrimonial, inclusive de carácter permanente se não for facultada à vítima a chave de desencriptação, possibilitando a recuperação por esta do controle dos dados ou do sistema, o Passo 5). Ainda a este propósito, cabe acentuar que o objetivo de obter "para si ou para outrem, vantagem econômica ilícita" integra apenas o elemento subjetivo do tipo.

No que respeita ao bem jurídico penalmente protegido, a própria redação do preceito aponta, em termos inequívocos, para o património da vítima. Aliás, no mesmo sentido, como antecipámos, da *Minuta* consta, explicitamente, que o "objetivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento de dados, cuja intenção seja a de efectuar uma transferência indevida de propriedade." (Ponto 36).

O que deverá ser entendido para além de uma consideração estática dos bens em propriedade, incluindo também todas as situações jurídicas de natureza patrimonial, além dos poderes de livre disposição das mesmas através de atos de natureza negocial. Consequentemente, a confiança dos operadores económicos dos mercados na integridade e fiabilidade nos sistemas e redes de computadores é também protegida, ainda que reflexamente.

---

[148] "Artigo 8º – Burla informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessária para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:

a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos;

b) De qualquer intervenção no funcionamento de um sistema informático,

com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.".

[149] "Artigo 8.º – Burla informática

Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de:

a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos;

b) Qualquer interferência no funcionamento de um sistema informático;

com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo."

Por outro lado, a referência a uma ação "não autorizada", pelo próprio titular do sistema ou pela lei, incluindo quem tivesse autorizado acesso ao sistema, embora não para a prática de tais ações, resultando na manipulação dos dados ou do sistema, obriga a considerar o controlo exclusivo destes também no âmbito dos bens jurídicos protegidos pelo crime de "Fraude informática".

Cabe ainda acrescentar que a tentativa, iniciada com o começo das ações mencionadas na previsão típica, será tendencialmente punível[150]. O mesmo não ocorrendo com os atos preparatórios[151].

3. Os concursos pensáveis

Como veremos em seguida, os vários Passos correspondentes aos ataques de *ramsonware* são suscetíveis de preencherem as previsões típicas de outros crimes constantes da *Convenção* para além da "Fraude informática", o que suscita necessariamente a questão dos concursos, embora não apenas com o tipo que identificámos como primário.

Todavia, para um tal exercício, apenas poderemos contar com os textos das previsões normativas e, sobretudo, com a consideração dos bens jurídicos protegidos, na falta de referências quanto às medidas das penas ou da atribuição das iniciativas processuais aos lesados e ou ao Ministério Público, cuja determinação caberá às Partes ao adequarem as respectivas leis à *Convenção*.[152]

a) com a "Violação de dados" (Artigo 4) **e** com a "Interferência em sistema" (Artigo 5)

Antes de mais, temos dois tipos cujos objetos e conteúdos das respetivas ações coincidem com os da "Fraude informática", pelo que os trataremos conjuntamente. Assim, no que se refere à "Violação de dados"[153], resulta que:

---

[150] Nos termos do previsto no Artigo 11 parágrafo 2, embora as Partes possam reservar-se o direito de não o fazer, conforme a parágrafo 3.

[151] Pois o crime correspondente ao "Uso indevido de aparelhagem" (Artigo 6) apenas prevê a obrigatoriedade para as Partes no que se refere aos tipos "Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador" e não aos "Crimes informáticos", como ocorre com a "Fraude informática" ou a "Falsificação informática", o mesmo valendo para os "Crimes relacionados ao conteúdo da informação" ou a "Violação de direitos autorais e de direitos correlatos".

[152] Sobre estas questões, tem um particular interesse o estudo, no contexto da *Convenção de Budapeste*, de P.D. VENÂNCIO (2013, 99-105), assim como, no âmbito do Direito português, embora desde perspectivas várias, mas quase sempre tendo por referência subjacente a *Convenção*, de D.R. NUNES (2017, 41-48), D.R. (2019, 69-82), assim como os contributos sintéticos, tendo por referência o crime de "Burla informática", de C.G. PEDRA (2019, 25-29), de C. RODRIGUES (2019, 54-60), de D.S. PALMA (2019, 86-89) e de P.L.R. MOTA (2019, 178-180).

[153] Manifestamente, esta terminologia não é feliz por coincidir com a usualmente usada, também no Brasil, para referir os incidentes de segurança conduzindo a violações de

"1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a danificação, a eliminação, a deterioração, a alteração ou a supressão dolosas e não autorizadas de dados de computador.

2. Qualquer Parte pode reservar-se o direito de exigir que da conduta descrita no parágrafo 1 resulte sério dano para a vítima."

A este propósito, quanto a uma questão de especial pertinência para o nosso objeto de estudo, ao corresponder ao Passo 1) dos ataques de *ransomware*, a *Minuta* esclarece que:

"A introdução de códigos dolosos, tais como vírus e rotinas tais como os chamados "cavalos de Tróia", encontra-se pois abrangida por este parágrafo da mesma maneira que a modificação dos dados resultante deste acto." (Ponto 61)

Por sua vez, a propósito da "Interferência em sistemas", temos que:

"Cada Parte adotará medidas legislativas semelhantes e outras providências necessárias para tipificar como crime, em sua legislação interna, qualquer grave obstrução ou impedimento, dolosos e não autorizados, do funcionamento de um sistema de computador por meio da inserção, transmissão, danificação, apagamento, deterioração, alteração ou supressão de dados de computador."

Sempre seguindo a *Minuta*, se na "Violação de dados" "[…] os interesses jurídicos protegidos são a integridade e o adequado funcionamento ou a correcta utilização dos dados ou programas informáticos armazenados." (Ponto 60), na "Interferência em sistemas", o mesmo "reside no interesse de operadores e utilizadores de sistemas informáticos e de telecomunicações em que os mesmos apresentem um funcionamento adequado." (Ponto 65).

Nestas bases, embora a consumação de cada um de estes crimes seja suscetível de afetar o património das vítimas, o mesmo não surge em primeira linha. Aliás, sobretudo no que se refere à "Interferência em sistemas", poderão estar em causa interesses sociais gerais, muito para além dos enunciados na *Minuta*. Sendo certo estarmos perante dois crimes de resultado e de dano, pois a respectiva consumação constitui um dano para o bem jurídico protegido.

---

segurança de dados pessoais, os "vazamentos de dados", conforme ao Artigo 48 da Lei n. 13.709, de 14 de agosto de 2018, a *Lei Geral de Proteção de Dados Pessoais*, sobre estas questões, por todos, M.D. MASSENO, G.M. MARTINS & J.L. FALEIROS Jr. (2020). Aliás, neste caso, a versão brasileira não apenas se afasta da oficiosa, a qual prefere a designação "Interferência nos dados", como da portuguesa e cabo-verdiana, "Dano provocado nos dados", sendo esta também objeto de críticas ao indiciar um mimetismo excessivo com o crime de "Dano", como também das oficiais "Data interference" e "Atteinte à l'intégrité des données".

Do mesmo modo, na respeitante ao elemento subjetivo de ambos os tipos, não está prevista qualquer intenção de natureza patrimonial, quer em prejuízo da vítima, quer em proveito próprio.

O que afastará a viabilidade de estarmos perante um concurso aparente, por consumpção, de estes tipos relativamente à "Fraude informática" no caso dos ataques de *ransomware*, embora seja pensável relativamente a outras condutas enquadráveis na previsão típica, como as transferências bancárias ilícitas[154].

Sem esquecer que as consequências dos ataques alcançam frequentemente bens jurídicos que extravasam acentuadamente o património das vítimas, mesmo quando os valores dos pagamentos exigidos são muito menores que os resultantes das interferências, muitas vezes atingindo a sociedade no seu conjunto. O que suscita ou a previsão legal de formas qualificadas de estes tipos ou o recurso a outros já presentes nos Ordenamentos penais, desde que passíveis de também aplicarem em meios digitais.

O que também permite ampliar a criminalização ao que seriam atos preparatórios dos ataques, por força do disposto a propósito do "Uso indevido de aparelhagem" (Artigo 6), não previsto para a "Fraude informática", como verificámos. Precisamente,

"1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas:

a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de:

i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5;

ii. uma senha de computador, código de acesso, ou dados similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e

b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize" […] [155]

---

[154] Sobre o *modus operandi* de estas, C.F. BARREIRA (2015), embora desde uma perspectiva diferente.

[155] O preceito acrescenta ainda que "[…]

b) com a "Falsificação informática" (Artigo 7)

Neste caso, também coincidem os objetos e os conteúdos das ações com os da "Fraude informática", embora restritamente aos dados, nos seguintes termos:

"Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento."[156]

Porém, diferem o não terem de ser dados alheios e o resultado consistente na obtenção de "dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem". O que configura um crime de perigo, ao não ser exigida a efetivação do dano.

Adicionalmente, a *Minuta* assume que:

"Neste caso, o interesse jurídico protegido será o da segurança e da credibilidade dos dados eletrónicos que poderão ter consequências ao nível das relações jurídicas." (Ponto 81, *in fine*).

O que extravasa também o âmbito patrimonial, alcançando o interesse geral relativo à segurança jurídica e a fiabilidade das transações eletrónicas, mesmo sem incidência económica.

Sempre no contexto dos ataques de *ransomware*, esta previsão abrangerá as condutas orientadas à produção de mensagens falsas de correio eletrónico, criadas com o objetivo de induzir as vítimas a ativarem programas que encriptarão dados, incluindo programas (*Phishing* e *Spear Phishing*), ou de páginas simuladas, de modo

2. Este Artigo não deve ser interpretado para estabelecer responsabilidade criminal quando a produção, venda, aquisição para uso, importação, distribuição ou disponibilização por qualquer meio ou a posse referidos no parágrafo 1 deste Artigo não se destine à prática de qualquer dos crimes tipificados de acordo com os artigos 2 a 5 desta Convenção, como para, por exemplo, a realização de testes autorizados ou a proteção de um sistema de computador.

3. Cada Parte pode reservar-se o direito de não aplicar o parágrafo 1 deste Artigo, desde que a reserva não se refira à venda, distribuição ou a disponibilização por qualquer meio, dos itens ou instrumentos referidos no parágrafo 1 a.ii deste Artigo.".

[156] Sobre a configuração de este tipo, também com referências à *Convenção*, embora essencialmente centrado nas fontes portuguesas, é de indicar o estudo de D.R. NUNES (2017).

a obterem as identificações e as palavras-passe das vítimas (*Pharming*), embora esta seja uma prática muito menos comum neste contexto[157].

Consequentemente, estaremos perante um concurso efetivo com a "Fraude informática", correspondendo a uma das vias para o Passo 1) dos ataques.

c) e ainda com o "Acesso ilegal" (Artigo 2)

Em cujos termos,

"Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador". [158]

Quanto ao bem jurídico protegido, ainda segundo a *Minuta*, está em causa

"A necessidade de protecção reflecte os interesses de organizações e indivíduos em gerir, operar e controlar os seus sistemas de forma livre e tranquila." (Ponto 44)

Por outras palavras, é procurada a segurança dos sistemas de computadores, de modo a manter a confiança dos particulares e das empresas, assim como dos mercados e da sociedade em geral, na respectiva segurança, confidencialidade e integridade, incluindo os dados presentes nos mesmos.

Em extrema síntese, será este um crime de perigo abstrato, não relevando qualquer dano ou dolo específico, designadamente de índole patrimonial.

Consequentemente, na perspectiva da "Fraude informática" em geral, apenas estaremos perante um concurso real se o acesso for obtido diretamente por meios técnicos (*Hacking*) ou através de *Pharming*, nos termos antes mencionados. Sendo ideal sempre que os ataques de *ransomware* se processem através de uma

---

[157] Para uma caraterização de ambas práticas, têm bastante interesse a exposição detalhada de C.F. BARREIRA (2015, 25-30), assim como as referências de D.R. NUNES (2019, 69-70).

[158] A propósito deste tipo, analisando as mudanças a resultarem da Convenção para *a Lei da Criminalidade Informática* então vigente em Portugal, a Lei n.º 109/91, de 17 de agosto <https://diariodarepublica.pt/dr/detalhe/lei/109-1991-674438>, têm muito interesse as considerações de R. BRAVO (2003), enquanto eu me ocupei da respetiva comparação com o previsto na Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa *a ataques contra os sistemas de informação* e que substitui a Decisão-Quadro 2005/222/JAI do Conselho <https://eur-lex.europa.eu/eli/dir/2013/40/oj?locale=pt> e com a *Lei Carolina Dieckmann*, Lei nº 12.737, de 30 de novembro de 2012*, dispõe sobre a tipificação criminal de delitos informáticos*; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> , M.D. MASSENO (2018b).

injeção de código malicioso, assim como nos casos de "inserção, alteração, apagamento ou supressão de dados de computador" ou de a "interferência no funcionamento de um computador ou de um sistema de computador" ser operada por quem estiver autorizado a aceder ao sistema, mas não a operar as referidas ações, sendo esta última via muito pouco comum.

4. Algumas, brevíssimas, considerações conclusivas

Nos próximos meses, cumprindo o previsto, o Congresso Nacional deverá adequar o brasileiro a este novo enquadramento. O que implicará uma reforma legislativa ampla e sistemática, inclusive reformulando intervenções recentes, como as introduzidas pela Lei nº 14.155, de 27 de maio de 2021, tendo por objeto realidades suscetíveis de caírem no âmbito da "Fraude informática" como a mesma está concebida na *Convenção*, com a tipificação da "Fraude eletrônica" e do "Furto mediante fraude"[159].

Em suma, embora o interesse expresso do Brasil estivesse sobretudo na Cooperação Internacional com as demais Partes da *Convenção*, surge agora uma oportunidade para atualizar também o seu Direito Penal Material. Espero ter dado um pequeno contributo para esse desiderato.

[159] Precisamente, esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>, sobre a mesma e suas dissonâncias com a Convenção, embora brevemente, M.D. MASSENO (2023b).

Referências bibliográficas:

BARREIRA, C.F. (2015). "Home banking: A Repartição dos prejuízos decorrentes de fraude informática". *RED – Revista Eletrónica de Direito*, 3. Disponível em: <https://bit.ly/4bbAD7h>.

BRAVO, R. (2003). "O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção". *Direito n@ Rede*, 3. Disponível em: <https://bit.ly/3tY2OWk>.

CARVALHO, F.P., MORALES G., O. & ÁLVAREZ F., M. (2018). "Regulamentação supranacional sobre Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como Paradigmas". *Actualidad Jurídica Uría Menéndez*, 48, 48-64. Disponível em: <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf >.

MASSENO, M.D. (2018a). *Os ataques de "Ransomware" na "Convenção de Budapeste" e no Direito Penal da União Europeia*. II Congresso Nacional de Direito Digital. Comissão de Direito Digital da Seção de Santa Catarina da Ordem dos Advogados do Brasil, Florianópolis. Disponível em: <https://bit.ly/48Ukuku>.

MASSENO, M.D. (2018b). "Da criminalização do "acesso ilícito" (*hacking*) nos Ordenamentos do Brasil e de Portugal". CALHEIROS, C. *et al*. (Eds.), *Direito na lusofonia : direito e novas tecnologias*. Braga: Escola de Direito da Universidade do Minho, 279-288. Disponível em: <https://bit.ly/3SfnC3L>.

MASSENO, M.D. (2023a). *Das Fontes Internacionais e Europeias da Cibercriminalidade*. Aula ao XII Curso de Mestrado em Direito e Informática da Escola de Direito da Universidade do Minho, Braga. Disponível em: <https://bit.ly/3U3XtYk>.

MASSENO, M.D. (2023b). *Os Tipos Penais Brasileiros perante a Convenção de Budapeste sobre o Cibercrime, principais problemas de adequação*. Porto Alegre: WB Educação. Disponível em: <https://bit.ly/46cuLXM>.

MASSENO, M.D., MARTINS, G.M. & FALEIROS Jr. (2020). "A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira". *Revista do CEJUR/TJSC: Prestação Jurisdicional*, 8(1), e346. Disponível em: <https://revistadocejur.tjsc.jus.br/cejur/article/view/346>.

MASSENO, M.D. & WENDT, E. (2017). "O *Ransomware* na Lei: Apontamentos Breves de Direito Português e Brasileiro". *Revista Eletrônica Direito & TI*, 1(8). Disponível em: <https://direitoeti.com.br/direitoeti/article/view/80>.

MOTA, P.L.R. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), *O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática*

(Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 167-192. Disponível em: <https://bit.ly/4aV3soa>.

NUNES, D.R. (2017). "O crime de falsidade informática". *JULGAR Online*. Disponível em: <https://julgar.pt/o-crime-de-falsidade-informatica/>.

NUNES, D.R. (2019). "O fenómeno do *Ransomware* e o seu enquadramento jurídico-penal". *Cyberlaw by CIJIC*, 8, 58-82. Disponível em: <https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_8.pdf >.

NUNES, D.R. (2019). "Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime". *Privacy and Data Protection Magazine - Revista Científica na Área Jurídica*, 5, 11-50. Disponível em: <https://www.europeia.pt/resources/media/documents/Revista_Privacy_Data_Protection_Magazine_N5.pdf>.

PALMA, D.S. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), *O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática* (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 73-105. Disponível em: <https://bit.ly/4aV3soa>.

PEDRA, C.G. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), *O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática* (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 11-38. Disponível em: <https://bit.ly/4aV3soa>.

PINTO, J.C. (2023). *Ransomware - Ameaça Crescente às Empresas*. Lisboa: Instituto Superior de Economia e Gestão da Universidade de Lisboa. Disponível em: <https://bit.ly/48PPrGC>.

RODRIGUES, C. (2019). "Crime de burla informática e nas comunicações. Enquadramento jurídico, prática e gestão processual". PEREIRA, L. M. C. S. *et al*. (Eds.), *O Crime de Abuso de Cartão de Garantia e Crédito e o Crime de Burla Informática* (Trabalhos do 2.º Ciclo do Curso de Formação – Ministério Público). Lisboa: Centro de Estudos Judiciários, 39-71. Disponível em: <https://bit.ly/4aV3soa>.

VENÂNCIO, P.D. (2013). "Similarity and Competition Between Cybercrimes Related to Computer Data in the Council of Europe's Convention on Cybercrime". *Masaryk University Journal of Law and Technology*, 7(1), 97-105. Disponível em: <https://journals.muni.cz/mujlt/article/view/2629>. Acesso em 30/01/2024.

VERDELHO, P. (2003). "A Convenção sobre Cibercrime do Conselho da Europa – Comentário". VERDELHO, P. *et al.* (Eds.): *Leis do Cibercrime*, I. Centro Atlântico: Vila Nova de Famalicão, 10-23. Disponível em: <https://bit.ly/3TUEM9r>.

Nota: todas as hiperligações foram verificadas no dia 30 de janeiro de 2024.

A Lei das Comunicações Eletrónicas & a Proteção das Pessoas Singulares no que diz Respeito ao Tratamento de Dados Pessoais e à Livre Circulação Desses Dados

D'joline Bragança Augusto[160]

Resumo

A lei das Comunicações Eletrónicas transpôs para a ordem jurídica interna as diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972. Porém, a nossa abordagem será numa vertente da existência, ou não, da proteção de dados da pessoa singular aquando do tratamento dos seus dados eletrónicos. Limitámos – nos às pessoas singulares devido ao RGPD aplicar -se apenas às pessoas singulares. Entender como são verdadeiramente tratados estes dados, como são designadas as pessoas singulares nesta realidade da comunicação eletrónica e, consequentemente, quais os procedimentos de processamento, intervenção, segurança e sanções será o enquadramento da Lei 16/2022. Neste contexto, abordaremos as diretivas (UE) 2018/1972 e 98/84/CE, pois, acreditamos serem de extrema importância no âmbito do conteúdo da Lei 16/2022. A acrescer, pretendemos fazer a nossa abordagem sempre na perspetiva do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016, pois, o foco aqui é perceber se as normas deste regulamento «estão a ser observadas» e, caso sim, «como e em que sentido é que estão a ser observadas» com a introdução de novas tecnologias, cuja internet tem sido o ponto mais alto para o risco elevado da perda de segurança da proteção dos dados das pessoas nas celebrações de contratos online e não só.

Palavras-chave: Princípios da transparência, Licitude; Direito à informação, limitação de dados; Direito ao apagamento (Direito ao esquecimento); Segurança.

[160] Mestranda em Direito Judiciário na Universidade Européia (Portugal), é Magistrada Judicial em Angola, cursou Direito na Universidade de Lisboa (Portugal) e Pós Graduação em Prevenção e intervenção em Violência Doméstica pela Cognos.pt; exerceu a função de Directora de Gabinete Adjunta do Provedor de Justiça (2007 – 2010) e a docência universitária no Curso de Direito na Universidade Gregório Semedo e no no ISIA (Instituto Superior)/Angola.

The Electronic Communications Law & the Protection of Individuals with Respect to the Processing of Personal Data and the Free Movement of Such Data

D'joline Bragança Augusto

Abstract

The Electronic Communications Law transposed directives 98/84/EC, 2002/77/CE and (EU) 2018/1972. However, our approach will be based on the existence, or not, of data protection for individuals when processing their electronic data,we limited ourselves to natural persons because the GDPR only applies to natural persons. Understanding how these data are truly processed, how natural persons are designated in this reality of electronic communication and, consequently, what processing, intervention, security and sanctions procedures are the framework of Law 16/2022.In this context, we will address directives (EU) 2018/1972 and 98/84/EC, as we believe they are extremely important within the scope of the content of Law 16/2022. Furthermore, we intend to always approach our approach from the perspective of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as the focus here is to understand whether the standards of this regulation "are being observed" and, if so, "how and in what sense are they being observed" with the introduction of new technologies, the internet of which has been the highest point for the high risk of loss of security in the protection of people's data in celebrations of online contracts and beyond.

Keywords: principles of transparency, lawfulness; Right to information, data limitation; Right to erasure (Right to be forgotten); Security

Introdução

A lei das Comunicações Eletrónicas, Lei nº. 16/2022 de 16 de Agosto, estabelece o regime jurídico aplicável às redes e serviços de comunicações eletrónicas, aos recursos e serviços conexos, à gestão do espectro de radiofrequências e dos recursos de numeração, bem como, a certos aspetos dos equipamentos terminais, e define as competências da autoridade reguladora nacional (ARN) e de outras autoridades competentes nestes domínios – Art.º 1.

Na verdade, ao ser resultado da transposição das diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972, esta tem, por um lado, como objetivo, assegurar a liberdade de oferta de serviços e redes de comunicações eletrónicas, mas, por outro lado, garantir a aplicação das medidas de restrições previstas no art.º 52, n.º 1 do Tratado sobre o Funcionamento da União Europeia (TFUE), mais concretamente, quanto à ordem pública, segurança pública e saúde pública[161]. Acrescemos ainda o facto desta Lei das Comunicações Eletrónicas, no âmbito da segurança pública, dispor de normas que garantem a limitação do tratamento de dados, de forma a respeitar e observar a essência dos direitos e liberdades do indivíduo (pessoa singular) constantes da Carta dos Direitos Fundamentais da União Europeia, especialmente, os seus Arts. 7.º, 8.º e 11.º, ressalvando ainda o Art.º 52, n.º 1, quanto ao princípio da proporcionalidade.

É assim que conseguimos perceber que no Art.º 2, nº.1, da Lei 16/2022 de 16 de Agosto – Lei das Comunicações Eletrónicas – o legislador começa imediatamente pela exclusão, ou seja, embora se aplique às pessoas singulares e coletivas, devido às especificidades que deve estritamente observar, começa por dispor qual o âmbito de exclusão:

> a) Os serviços da sociedade da informação, definidos no Decreto -Lei n.º 30/2020, de 29 de junho, que não consistam num serviço de comunicações eletrónicas;
>
> b) Os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas, incluindo os serviços de programas televisivos e de rádio e os serviços de audiotexto e de valor acrescentado baseados no envio de mensagem;

[161] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho de 11 de Dezembro de 2018 – Código Europeu das Comunicações Eletrónicas – considerandos 5, 6.

c) As redes privativas do Ministério da Defesa Nacional, ou sob sua responsabilidade, e das forças e serviços de segurança e de emergência, as quais se regem por legislação específica;

d) A rede informática do Governo, gerida pelo Centro de Gestão da Rede Informática do Governo, bem como as redes criadas para prosseguir os fins previstos na alínea g) do n.º 2 do artigo 2.º do Decreto -Lei n.º 16/2012, de 26 de janeiro.»

É nosso entendimento que o âmbito de aplicação constante do Art.º 2, n.º 2, deve ser lido em consonância com o Art.º 3, pois, independentemente do Art.º 1 dispor acerca do objeto da presente Lei, é o Art.º 3 que vai "decifrar" os conceitos específicos e inerentes à própria Lei das Comunicações Eletrónicas, pelo que, embora de forma extensiva, acreditamos ser útil fazer esta explicação, primeiramente do âmbito de aplicação e, posteriormente, dos conceitos constantes da Lei em apreço.

Âmbito de aplicação – Art. 2º, n.º 2:

«a) O regime da disponibilização no mercado, da colocação em serviço e da utilização de equipamentos de rádio, aprovado pelo Decreto -Lei n.º 57/2017, de 9 de junho;

b) O regime aplicável à construção de infraestruturas aptas ao alojamento de redes de comunicações eletrónicas, à instalação de redes de comunicações eletrónicas e à construção de infraestruturas de telecomunicações em loteamentos, urbanizações, edifícios e conjuntos de edifícios, previsto no Decreto -Lei n.º 123/2009, de 21 de maio;

c) O regime aplicável à utilização do espectro de radiofrequências, incluindo as condições relativas às redes e estações de radiocomunicações, previsto no Decreto -Lei n.º 151 -A/2000, de 20 de julho, em tudo o que não for especialmente previsto na presente lei;

d) O regime jurídico aplicável aos radioamadores, previsto no Decreto -Lei n.º 53/2009, de 2 de março;

e) O regime jurídico aplicável aos serviços públicos essenciais, previsto na Lei n.º 23/96, de 26 de julho;

f) O regime jurídico aplicável à prestação de serviços de promoção, informação e apoio aos consumidores e utentes através de centros telefónicos de relacionamento (call centers), aprovado pelo Decreto -Lei n.º 134/2009, de 2 de junho,»

Nestes termos, para melhor entendimento, no seu Art.º 3, com a epígrafe denominada "Definições", o legislador atribuiu uma definição taxativa a cada conceito específico utilizado na própria Lei.

1. Regulamento (EU) 2016 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Trata-se de um Regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Tal como temos uma União Europeia que prima pela livre circulação de pessoas e bens, também procura -se que os dados de pessoas singulares, embora circulem de forma livre, tenham um tratamento que os proteja.

Sobre o impacto do RGPD, diz o Professor António Menezes Cordeiro que este trouxe uma "*densificação dos direitos dos titulares de dados pessoais, o agravamento dos deveres dos responsáveis pelo tratamento de dados e dos subcontratantes, o reforço das competências das autoridades de controlo ou a obrigatoriedade de designação de encarregados de proteção de dados*"[162].

A corroborar tal afirmação estão as próprias normas e considerandos do Regulamento, onde, no considerando 1 expressamente dispõe que "*a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental,* fundamentando com base nos artigos 8.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia e 16.º, n.º 1 do Tratado sobre o Funcionamento da União Europeia (TFUE).

Ainda quanto à liberdade da circulação dos dados pessoais, o considerando 2 dispõe que os princípios e regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local da residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente, o direito à proteção de dados.

[162] A. Barreto Menezes Cordeiro, "Direito da Proteção de Dados" à Luz do RGPD e da Lei n.º 58/2019, Almedina, 2020, pág. 29 e 30.

No entanto, este direito fundamental não é absoluto, sendo que podemos ver no considerando 4 que "o direito à proteção de dados deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais". Todo este nível de exigência para se garantir que a recolha e partilha de dados sejam feitas num contexto de segurança jurídica.

E é aqui que entramos na questão das comunicações eletrónicas, pois, estão ligadas às novas tecnologias. Reparemos que no considerando 6 do RGPD refere-se exatamente à rápida evolução da tecnologia e a sua globalização de tal modo que criaram novos desafios em matéria de proteção de dados pessoais.

O facto das novas tecnologias permitirem que empresas e entidades públicas utilizem os dados pessoais numa escala sem precedentes, bem como, das pessoas singulares disponibilizarem cada vez mais as suas informações pessoais de uma forma pública e global, foi uma das razões pela qual se aprovou este Regulamento (EU) 2016/679, pois, esta grande evolução leva inclusive à transferência de dados pessoais para países terceiros (em relação à União Europeia) e Organizações Internacionais. Mais uma vez: a necessidade de uma proteção devida e com segurança jurídica.

Como é que se previu?

Primeiramente pelos princípios: quando é o próprio Regulamento a estipular os princípios específicos pelas quais se devem pautar, sempre, durante o tratamento de dados de pessoas singulares, significa dizer que aquando da aplicação de qualquer norma, os princípios inerentes à este direito fundamental devem sempre ser tidos em conta.

Assim, constituem princípios relativos ao tratamento de dados pessoais:

Licitude – artº 5/1, al a) e 6.º - conseguimos ver em consonância com o considerando **39** que o tratamento de dados pessoais deverá ser feito de forma lícita e equitativa, no sentido de ser transparente para as pessoas singulares. E é aqui que chamo à colação o Princípio da **Transparência** que estando em harmonia, a transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão e formuladas numa linguagem clara e simples[3]. Gostaria de aqui fazer uma ligação com a nossa Lei 16/2022 de 16 de Agosto que sendo resultado da transposição de três diretivas, conforme acima já mencionado, a mesma prevê este princípio da Licitude e Transparência

relativamente ao uso das comunicações eletrónicas no seu art-º 6, fazendo menção ainda aos princípios da imparcialidade, não discriminação, objetividade, tempestividade e proporcionalidade.

Limitação das finalidades – art.º 5/1 al b) - é de notar que os dados são recolhidos para uma finalidade determinada, explícita e legítima, sendo que não podem ser tratados posteriormente de uma forma incompatível com essas finalidades. Existem exceções quanto à possibilidade destes dados poderem ser tratados posteriormente: nos casos de tratamento posterior para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos.

Minimização dos dados -, art.º 5/ 1 al c) - estes têm de ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para quais os dados são tratados.

Exatidão – art.º 5/1 al d) – trata – se dos dados a serem tratados serem exatos e atualizados sempre que necessário. Este princípio é que vai permitir que todos os dados inexatos, tendo em atenção às finalidades para os quais estão a ser tratados, sejam apagados ou retificados sem demora.

Limitação da conservação – art.º 5/1 al e) – há que ter sempre em conta a finalidade para qual os dados pessoais estão ser tratados. É consoante esta finalidade que se terá em conta o período necessário para sua conservação. A segunda parte deste artigo refere os casos de exceção, casos em que a conservação pode ser feita por períodos mais longos: quando sejam tratados exclusivamente para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos.

Integridade e confidencialidade – art.º 5/ 1 al f) – este princípio tem que ver com a garantia da segurança no tratamento dos dados pessoais, incluindo aqui situações de tratamentos de dados não autorizados ou ilícitos, contra a sua perda, destruição ou danificação acidental. São nestes termos adotadas medidas adequadas.

Responsabilidade – art.º 5/2 – trata -se do princípio aplicável à pessoa responsável pelo tratamento do titular dos dados pessoais. Aquele deve observar todos os trâmites aquando do tratamento dos dados pessoais.

Para além disso, enquanto que na Lei 16/2022 de 16 de Agosto se faz menção a uma Autoridade de Regulação que é a ANACOM, no que respeita à proteção de dados em Portugal é a Comissão Nacional de Proteção de Dados (NCPD) que age com independência na prossecução das suas atribuições e competências, previstas designadamente nos artigos 57.º da RGPD, 6.º da Lei 58/2019 e 44.º da Lei 59/2019: controlar e executar a aplicação da Lei; promover, sensibilizar e informar; aconselhar as autoridades nacionais e acompanhar a evolução do Direito da proteção de Dados. A CNPD é composta por sete membros: o Presidente da República (eleito pela Assembleia da República), sendo que são eleitos mais dois vogais pela Assembleia da República, um vogal é designado pelo Conselho Superior da Magistratura, outro vogal é designado pelo Conselho Superior da Magistratura do Ministério Público e o Governo designa dois vogais.

Estamos assim perante uma autoridade de controlo designada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 e que a nível interno, à luz da Lei n.º 58/2019, veio impor a designação de um Fiscal Único, designado pela Assembleia da República, a quem cabe controlar a legalidade, a regularidade e a boa gestão financeira e patrimonial da CNPD, nos termos previstos no art.º 19 – A da Lei Orgânica da CNPD. Ou seja, este Regulamento criou um processo de autorregulação para garantir o legal tratamento de dados pessoais na União Europeia. Isto quer dizer que, no caso de Portugal, as empresas deixaram de ficar dependentes de uma decisão da CNPD para fazer o tratamento de dados. Agora são as próprias empresas que têm de provar que estão a aplicar o regulamento e cabe à Comissão, ou outro organismo designado como fiscalizador, avaliar esse comportamento.

Esta comparação pensamos ser importante para demonstrar o referido impacto que a proteção de dados tem tido, pretendendo o legislador com medidas tão restritas inerentes à este tratamento, criar uma consciencialização às pessoas quando estão a fazer uso dos seus dados pessoais perante tecnologias, como por exemplo a internet.

2 - Acórdão do Tribunal de Justiça (Quarta Secção) 27 de outubro de 2022 (*)[163].

Estamos perante o processo **C-129/21** que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo **267.º TFUE**, pelo *hof van beroep te Brussel* (Tribunal de Recurso de Bruxelas, Bélgica), por Decisão de 24 de fevereiro de 2021, que deu entrada no Tribunal de Justiça em 2 de março de 2021, no processo *Proximus NV* contra *Gegevensbeschermingsautoriteit*.

O pedido de decisão prejudicial tem por objeto a interpretação do artigo 12.º, n.º 2, lido em conjugação com o artigo 2.º, segundo parágrafo, alínea f), da Diretiva 2002/58/CE[10] do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11) (a seguir «Diretiva 2002/58»), bem como do artigo 5.º, n.º 2, e dos artigos 17.º, 24.º e 95.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1, a seguir «RGPD»).

Este pedido foi apresentado no âmbito de um litígio que opõe a Proximus NV, sociedade de direito público belga, à Gegevensbeschermingsautoriteit (Autoridade de proteção de dados, Bélgica) (a seguir «APD»), a respeito da decisão pela qual a Geschillenkamer van de Gegevensbeschermingsautoriteit (Secção de Contencioso da APD, a seguir «Secção de Contencioso») aplicou à Proximus medidas corretivas e uma coima de 20.000 euros por violação de várias disposições do RGPD.

A Proximus, prestadora de serviços de telecomunicações na Bélgica, fornece igualmente listas telefónicas e serviços de informação telefónica acessíveis ao público (a seguir «listas»), em conformidade com as disposições da Lei Relativa às

163
https://curia.europa.eu/juris/document/document.jsf?text=&docid=267605&pageIndex=0&doclang=PT& mode=lst&dir=&occ=first&part=1&cid=6477940

Comunicações Eletrónicas. Estas listas contêm o nome, o endereço e o número de telefone (a seguir «dados de contacto») dos assinantes dos diferentes fornecedores de serviços telefónicos acessíveis ao público (a seguir «operadores»). Existem outras listas publicadas por terceiros.

Os dados de contacto desses assinantes são regularmente comunicados à Proximus pelos operadores, com exceção dos dados de contacto dos assinantes que manifestaram o desejo de não figurar nas listas editadas pela Proximus. Na Bélgica, a distinção entre os assinantes que pretendem figurar numa lista e os que não o desejam fazer traduz-se, na prática, pela atribuição de um código no registo de cada assinante, concretamente, «NNNNN», para os assinantes cujos dados de contacto podem aparecer, e «XXXXX» para os assinantes cujos dados de contacto permanecem confidenciais. A Proximus transmite igualmente as coordenadas que recebe a outro fornecedor de listas telefónicas.

O autor da reclamação é um assinante da operadora de serviços telefónicos Telenet, que opera no mercado belga. A Telenet não fornece listas, mas transmite as coordenadas dos seus assinantes a fornecedores de listas, nomeadamente à Proximus.

Em 13 de janeiro de 2019, este assinante pediu à Proximus que não incluísse os seus dados de contacto nas listas editadas tanto pela Proximus como por terceiros. Na sequência deste pedido, a Proximus alterou o estatuto deste assinante no seu sistema informático para que os dados de contacto do referido assinante deixassem de ser tornados públicos.

Em 31 de janeiro de 2019, a Proximus recebeu da Telenet uma atualização periódica dos dados dos assinantes desta última. Esta atualização continha novos dados do assinante em causa, que não estavam indicados como confidenciais. Estas informações foram objeto de tratamento automatizado pela Proximus, foram registadas, e passaram novamente a figurar nas listas desta última.

Em 14 de agosto de 2019, após ter verificado que o seu número de telefone tinha sido publicado nas listas da Proximus e de terceiros, o assinante em causa pediu novamente à Proximus que não incluísse os seus dados nessas listas. No mesmo dia, a Proximus respondeu ao autor da reclamação que tinha suprimido os seus dados das listas e contactado a Google para que as hiperligações pertinentes para o sítio Internet da Proximus fossem suprimidas. A Proximus informou igualmente este

assinante de que tinha transmitido os seus dados de contacto a outros fornecedores de listas e que, graças às atualizações mensais, esses fornecedores tinham sido informados do pedido do autor da reclamação.

Ao mesmo tempo, o referido assinante apresentou uma queixa à APD contra a Proximus com fundamento na circunstância de o seu número de telefone aparecer em algumas dessas listas apesar do seu pedido no sentido de os seus dados de contacto não serem incluídos nas mesmas.

Em 5 de setembro de 2019, o assinante em causa e a Proximus voltaram a trocar mensagens a respeito da publicação dos dados desse assinante na lista de um terceiro. Neste contexto, a Proximus sublinhou que transmite os dados de contacto dos seus assinantes a outros fornecedores de listas, mas que desconhece os procedimentos de funcionamento interno desses fornecedores.

Em 30 de julho de 2020, após um processo contraditório, a Secção de Contencioso adotou uma decisão pela qual aplicou à Proximus medidas corretivas e uma coima no montante de 20 000 euros por violação, nomeadamente, do artigo 6.º do RGPD, conjugado com o artigo 7.º deste regulamento, e do artigo 5.º, n.º 2, do referido regulamento, lido em conjugação com o artigo 24.º deste último. Em especial, em primeiro lugar, ordenou à Proximus que desse seguimento adequado e imediato à retirada do consentimento do assinante em causa e que respeitasse os pedidos desse assinante destinados a exercer o seu direito ao apagamento dos dados que lhe diziam respeito. Em seguida, ordenou à Proximus que tomasse as medidas técnicas e organizacionais adequadas para assegurar que os tratamentos dos dados pessoais que efetua sejam conformes com as disposições do RGPD. Por último, ordenou à Proximus que deixasse de transmitir ilicitamente esses dados a outros fornecedores de listas.

Em 28 de agosto de 2020, a Proximus interpôs recurso desta decisão para o hof van beroep te Brussel (Tribunal de Recurso de Bruxelas, Bélgica).

Segundo a Proximus, em conformidade com o artigo 45.º, n.º 3, da Lei Relativa às Comunicações Eletrónicas, o consentimento do assinante não é exigido, sendo que incumbe aos próprios assinantes pedir para não figurar nas listas segundo um sistema dito de *«opt-out»*. Na falta desse pedido, o assinante em causa pode efetivamente figurar nessas listas. Por este motivo, segundo a Proximus, no caso

em apreço o assinante não tinha de dar nenhum «consentimento» na aceção da Diretiva 95/46 ou do RGPD.

De opinião contrária, a APD alegou, em substância, que o artigo 12.º, n.º 2, da Diretiva 2002/58 e o artigo 133.º, n.º 1, da Lei Relativa às Comunicações Eletrónicas exigem o «consentimento dos assinantes», na aceção do RGPD, para que os fornecedores de listas possam tratar e transmitir os seus dados pessoais.

O órgão jurisdicional de reenvio considera que a Diretiva 2002/58 constitui uma *lex specialis* em relação ao RGPD, como confirmam o considerando 173 e o artigo 95.º do RGPD. Por conseguinte, nas situações em que a Diretiva 2002/58 precisa as regras do RGPD, as disposições específicas desta diretiva prevalecem, enquanto *lex specialis*, sobre as disposições mais gerais do RGPD.

Neste contexto, o órgão jurisdicional de reenvio observa que o artigo 12.º, n.º 2, da Diretiva 2002/58 e o artigo 133.º, n.º 1, da Lei Relativa às Comunicações Eletrónicas, embora exijam uma expressão de vontade dos assinantes para que os fornecedores de listas possam tratar os seus dados pessoais, não especificam se esta expressão de vontade se deve traduzir no exercício de um direito de opção, como sustenta a Proximus, ou na manifestação de um verdadeiro consentimento, na aceção do RGPD, como indica a APD. Quanto a este ponto, o órgão jurisdicional de reenvio sublinha que a jurisprudência do Tribunal de Justiça, em especial o Acórdão de 5 de maio de 2011, Deutsche Telekom (C-543/09, EU:C:2011:279, n.º 61), estabeleceu que, como decorre de uma interpretação contextual e sistemática do artigo 12.º da Diretiva 2002/58, a expressão de vontade em causa corresponde a um «consentimento» que se refere à finalidade da publicação dos dados pessoais numa lista pública e não à identidade de um fornecedor de listas em particular.

Além disso, uma vez que não foi estabelecido nenhum regime específico relativo à retirada dessa expressão de vontade ou desse «consentimento» por um assinante, nem na Diretiva 2002/58, nem na Lei Relativa às Comunicações Eletrónicas, nem num decreto de execução, o órgão jurisdicional de reenvio interroga-se sobre a questão de saber se todas as disposições do RGPD devem ser aplicadas automaticamente e sem restrições igualmente no contexto concreto das listas telefónicas.

Nestas condições, o hof van beroep te Brussel (Tribunal de Recurso de Bruxelas) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

> 1) Deve o artigo 12.º, n.º 2, da Diretiva 2002/58[/CE], lido em conjugação com o artigo 2.º, alínea f), da referida diretiva e com o artigo 95.º do [RDPG], ser interpretado no sentido de que permite que uma autoridade de controlo nacional, na falta de disposições em contrário da legislação
>
> nacional, exija o "consentimento" do assinante, na aceção do [RGPD],
>
> como fundamento para a publicação dos seus dados pessoais em listas telefónicas e serviços de informação telefónica públicos, tanto dos que são publicados pelo próprio operador como dos que são publicados por terceiros fornecedores?
>
> 2) Deve o direito ao apagamento dos dados previsto no artigo 17.º do [RGPD] ser interpretado no sentido de que se opõe a que uma autoridade de controlo nacional qualifique o pedido de um assinante para ser removido das listas telefónicas e dos serviços de informação públicos de pedido de apagamento dos dados na aceção do artigo 17.º do [RGPD]?
>
> 3) Devem os artigos 24.º e 5.º, n.º 2, do [RGPD] ser interpretados no sentido de que se opõem a que uma autoridade de controlo nacional infira da responsabilidade aí consagrada que o responsável pelo tratamento deve adotar as medidas técnicas e [organizacionais] que forem razoáveis para informar os terceiros responsáveis pelo tratamento — a saber, o fornecedor de serviços telefónicos e outros fornecedores de listas telefónicas e de serviços de informação telefónica que recebam dados desse responsável pelo tratamento — sobre a revogação do consentimento pelo particular, em conformidade com o artigo 6.º, em conjugação com o artigo 7.º do [RGPD]?
>
> 4) Deve o artigo 17.º, n.º 2, do [RGPD] ser interpretado no sentido de que se opõe a que uma autoridade de controlo nacional ordene a um fornecedor de listas telefónicas e de serviços de informação telefónica públicos, ao qual tenha sido solicitado que deixe de divulgar os dados de determinada pessoa,

que tome medidas razoáveis para informar os motores de busca sobre esse pedido de apagamento dos dados?

A Proximus alega que o processo principal não tem por objeto a publicação, por um operador de serviços telefónicos, de listas que contêm dados pessoais, pelo que a primeira questão prejudicial deve ser considerada inadmissível por dizer respeito a tal caso.

Segundo jurisprudência constante, as questões relativas à interpretação do direito da União submetidas pelo juiz nacional no quadro regulamentar e factual que define sob a sua responsabilidade, e cuja exatidão não cabe ao Tribunal de Justiça verificar, gozam de uma presunção de pertinência. O Tribunal de Justiça só pode recusar pronunciar-se sobre um pedido apresentado por um órgão jurisdicional nacional se for manifesto que a interpretação do direito da União solicitada não tem nenhuma relação com a realidade ou com o objeto do litígio no processo principal, quando o problema for hipotético ou ainda quando o Tribunal de Justiça não dispuser dos elementos de facto e de direito necessários para dar uma resposta útil às questões que lhe são submetidas (Acórdão de 1 de agosto de 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, n.º 48 e jurisprudência referida).

No presente caso, o litígio no processo principal é apenas entre uma pessoa singular e uma empresa, que não é o seu operador de serviços telefónicos, relativamente ao modo como essa empresa tratou os dados pessoais dessa pessoa no contexto da publicação de listas. Daqui resulta que a primeira questão é inadmissível na medida em que busca uma interpretação das exigências decorrentes do artigo 12.º, n.º 2, da Diretiva 2002/58 caso seja o próprio operador de serviços telefónicos dessa pessoa a publicar os seus dados pessoais em listas.

Decorre do exposto que, com a sua primeira questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 12.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 2.º, segundo parágrafo, alínea f), desta diretiva e com o artigo 95.º do RGPD, deve ser interpretado no sentido de que é exigido o «consentimento», na aceção do artigo 4.º, ponto 11, do RGPD, do assinante de um operador de serviços telefónicos para que os seus dados pessoais figurem em listas publicadas por fornecedores diferentes desse operador.

Para responder a esta questão, importa recordar que, nos termos do seu artigo 1.º, n.º 1, a Diretiva 2002/58 prevê, nomeadamente, a harmonização das disposições nacionais necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, em particular do direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas.

A este respeito, há que recordar que resulta do artigo 12.º, n.º 1, desta diretiva, bem como do seu considerando 38, que os assinantes, antes de serem inscritos em listas públicas, são informados dos fins para os quais estas são elaboradas e de qualquer utilização particular que delas possa ser feita, nomeadamente através das funções de procura incorporadas em versões eletrónicas das listas.

O considerando 39 da referida diretiva precisa, em seguida, no que respeita à obrigação de informação prévia dos assinantes ao abrigo do seu artigo 12.º, n.º 1, que, «[n]os casos em que os dados [pessoais] possam ser transmitidos a um ou mais terceiros, o assinante deverá ser informado desta possibilidade e do destinatário ou das categorias de possíveis destinatários».

Após ter obtido as informações referidas no artigo 12.º, n.º 1, da Diretiva 2002/58, o assinante pode, como resulta do n.º 2 do mesmo artigo, decidir se os seus dados pessoais, e quais desses dados, devem figurar numa lista pública.

Como já decido pelo Tribunal de Justiça, tal informação prévia permite que o assinante consinta na publicação dos seus dados pessoais em listas públicas, sendo que esse consentimento é necessário para efeitos dessa publicação (ver, neste sentido, Acórdão de 5 de maio de 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, n.ºs 54 e 58).

A exigência de obtenção do consentimento do assinante em causa para efeitos da publicação desses dados em listas é confirmada pelo artigo 12.º, n.º 3, da Diretiva 2002/58, nos termos do qual os Estados-Membros poderão exigir que «o consentimento adicional dos assinantes seja solicitado» para qualquer utilização de uma lista pública que não a busca de coordenadas das pessoas com base no nome.

Todavia, como o Tribunal de Justiça precisou, resulta de uma interpretação contextual e sistemática do artigo 12.º da Diretiva 2002/58 que o consentimento a

título do n.º 2 deste artigo se refere à finalidade da publicação de dados pessoais numa lista pública e não à identidade de um fornecedor de listas em particular. Deste modo, quando esse assinante tiver consentido que os seus dados sejam publicados numa lista com uma finalidade específica, não terá geralmente interesse em opor-se à publicação dos mesmos dados noutra lista semelhante (Acórdão de 5 de maio de 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, n.ºs 61 e 62).

A este respeito, o considerando 39 desta diretiva confirma que a transmissão de dados pessoais dos assinantes a terceiros é permitida na «condição de que os dados não possam ser utilizados para outros fins diferentes dos que motivaram a sua recolha».

Daqui resulta que, quando um assinante tenha sido informado por um operador de serviços telefónicos, como a Telenet, da possibilidade de transmissão dos seus dados pessoais a uma terceira empresa, como a Proximus ou outros terceiros, tendo em vista a sua publicação numa lista pública, e esse assinante tenha consentido na publicação desses dados em tal lista, a transmissão por esse operador ou empresa desses mesmos dados a outra empresa para fins de publicação de uma lista pública impressa ou eletrónica, ou de disponibilização dessas listas para consulta através de serviços de informações, não tem de estar sujeita a novo consentimento por parte desse assinante, se se garantir que os dados em causa não serão utilizados para fins diferentes daqueles para os quais foram recolhido com vista à sua primeira publicação. Com efeito, o consentimento, nos termos do artigo 12.º, n.º 2, da Diretiva 2002/58, de um assinante devidamente informado, para a publicação dos seus dados pessoais numa lista pública refere-se à finalidade dessa publicação e é assim extensivo a qualquer tratamento posterior dos referidos dados por parte de empresas terceiras que operam no mercado dos serviços de informação telefónica acessíveis ao público e dos serviços de listas, desde que esses tratamentos prossigam essa mesma finalidade (Acórdão de 5 de maio de 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, n.º 65).

Em contrapartida, como enuncia o considerando 39 desta diretiva, se a parte que recolhe os dados a partir do assinante ou de terceiros a quem os mesmos tenham sido transmitidos pretender utilizá-los para outro fim, quer a parte que

recolheu os dados, quer o terceiro a quem foram transmitidos, terá de obter novo consentimento do assinante.

No que respeita às modalidades segundo as quais esse consentimento deve ser manifestado, resulta do artigo 2.º, segundo parágrafo, alínea f), da Diretiva 2002/58, lido em conjugação com o artigo 94.º, n.º 2, e com o artigo 95.º do RGPD, que esse consentimento deve, em princípio, cumprir as exigências resultantes do artigo 4.º, ponto 11, deste regulamento.

No caso em apreço, o artigo 4.º, ponto 11, do RGPD, disposição aplicável aos factos em causa no processo principal, define o «consentimento do titular dos dados» no sentido de que exige uma manifestação de vontade, «livre, específica, informada e inequívoca», pela qual o titular dos dados aceita, mediante declaração ou «ato positivo inequívoco», que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Daqui decorre que esse consentimento é necessário para que os dados pessoais do assinante de um operador de serviços telefónicos possam figurar em listas.

Por conseguinte, a publicação dos dados pessoais do assinante em questão em listas como as editadas pela Proximus ou por outros fornecedores só pode ser considerada lícita, na aceção do artigo 6.º, n.º 1, alínea a), do RGPD, se tal consentimento foi expressamente dado ao operador de serviços telefónicos ou a um desses fornecedores de listas.

Dito isto, como foi recordado no n.º 49 do presente acórdão, esse consentimento não pressupõe que, à data em que o mesmo é dado, a pessoa em causa conhece necessariamente a identidade de todos os fornecedores de listas que tratarão os seus dados pessoais.

Tendo em conta as considerações precedentes, há que responder à primeira questão que o artigo 12.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 2.º, segundo parágrafo, alínea f), desta diretiva e com o artigo 95.º do RGPD, deve ser interpretado no sentido de que é exigido o «consentimento», na aceção do artigo 4.º, ponto 11, do RGPD, do assinante de um operador de serviços telefónicos para que os dados pessoais desse assinante figurem nas listas publicadas por fornecedores diferentes desse operador, podendo esse consentimento ser dado quer ao referido operador quer a um dos seus fornecedores.

Quanto a segunda questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 17.º do RGPD deve ser interpretado no sentido de que o pedido de um assinante destinado à supressão dos seus dados pessoais das listas constitui um exercício do «direito ao apagamento», no sentido deste artigo.

Antes de mais, há que salientar que a Proximus alega que o artigo 17.º do RGPD não é aplicável a um fornecedor de listas que, como no caso em apreço, não é o operador de serviços telefónicos do assinante e que um pedido, como o mencionado no número anterior do presente acórdão, deveria, quando muito, ser considerado um pedido de retificação, no sentido do artigo 16.º deste regulamento, pelo que a segunda questão prejudicial é inadmissível por falta de pertinência para o processo principal.

Todavia, os argumentos assim avançados por esta parte dizem respeito, em substância, ao âmbito de aplicação e ao alcance e, portanto, à interpretação, das disposições do direito da União sobre as quais incide a segunda questão. Ora, assim sendo, tais argumentos, que dizem respeito ao mérito da questão submetida, não podem, por natureza, conduzir à inadmissibilidade da mesma (Acórdão de 13 de janeiro de 2022, Minister Sprawiedliwości, C-55/20, EU:C:2022:6, n.º 83).

Daqui resulta que a segunda questão prejudicial é admissível.

Em primeiro lugar, importa sublinhar que, em virtude do artigo 12.º, n.º 2, segundo período, da Diretiva 2002/58, os assinantes devem ter, nomeadamente, a possibilidade de obter a supressão dos seus dados pessoais das listas públicas.

Todavia, a concessão dessa possibilidade aos assinantes não constitui uma obrigação específica, na aceção do artigo 95.º do RGPD, a que os fornecedores de listas estejam sujeitos e que permita excluir a aplicação das disposições pertinentes deste regulamento. Com efeito, como salientou, em substância, o advogado-geral, no n.º 54 das suas conclusões, a Diretiva 2002/58 não contém indicações a respeito das modalidades, execução e consequências dos pedidos de supressão dos dados pessoais. Por este motivo, como resulta, por outro lado, do considerando 10 desta diretiva, lido em conjugação com o artigo 94.º deste regulamento, as disposições do RGPD podem ser aplicadas nessa situação.

Em segundo lugar, decorre do artigo 17.º, n.º 1, alíneas b) e d), do RGPD, que a pessoa em causa tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais e que o responsável pelo tratamento tem a obrigação de apagar esses dados sem demora injustificada, nomeadamente quando o titular «retira o consentimento em que se baseia o tratamento nos termos do artigo 6.º, n.º 1, alínea a), […] e se não existir outro fundamento jurídico para o referido tratamento» ou ainda quando «[o]s dados pessoais foram tratados ilicitamente».

A este respeito, por um lado, decorre da resposta à primeira questão prejudicial que a publicação dos dados pessoais de um assinante em listas assenta no consentimento desse assinante.

Por outro lado, resulta do artigo 6.º, n.º 1, alínea a), e do artigo 7.º, n.º 3, do RGPD, que esse consentimento constitui uma das condições necessárias para concluir pela licitude do tratamento dos dados pessoais do assinante em causa e que esse consentimento pode ser retirado a qualquer momento e segundo modalidades tão simples como as que permitiram ao titular dar esse consentimento.

No caso em apreço, quando o assinante pede que os seus dados já não constem de uma lista, retira o seu consentimento para a publicação desses dados.

Com base na retirada do seu consentimento, e na falta de outros fundamentos jurídicos para esse tratamento, adquire o direito de pedir o apagamento dos seus dados pessoais dessa lista, nos termos do artigo 17.º, n.º 1, alínea b), do RGPD ou, no caso de o responsável pelo tratamento continuar a publicar os referidos dados de maneira ilícita, em virtude do artigo 17.º, n.º 1, alínea d), deste regulamento.

Nestas condições, há que considerar que o pedido de um assinante destinado à supressão dos seus dados pessoais das listas pode ser considerado um exercício do

«direito ao apagamento» dos referidos dados, na aceção do artigo 17.º do RGPD.

Esta conclusão não pode ser posta em causa pelo argumento invocado pela Proximus segundo o qual se deve considerar que o referido pedido se destina a permitir que o assinante exerça o seu direito de obter, por parte do responsável pelo tratamento, a retificação dos dados pessoais que lhe digam respeito a título do

artigo 16.º do RGPD. Com efeito, nos termos desta disposição, essa retificação é possível quando os dados pessoais são inexatos e destina-se a permitir que o seu titular consiga que os mesmos sejam completados.

Ora, no caso em apreço, um pedido de supressão dos dados de um assinante que figura numa lista não visa substituir dados inexatos por dados corretos ou completar dados incompletos, mas sim suprimir a publicação de dados corretos.O facto de, no caso em apreço, essa supressão se traduzir na simples alteração do código que é atribuído ao assinante em causa na base de dados da Proximus, base essa a partir da qual os dados pessoais deste assinante são publicados nas listas, não impede que um pedido de supressão dos dados pessoais que figuram nessas listas seja considerado um «pedido de apagamento», na aceção do artigo 17.º do RGPD. Com efeito, como resulta dos autos submetidos ao Tribunal de Justiça, a modalidade de supressão prevista pelo referido operador constitui uma medida de natureza puramente técnica ou organizacional necessária para dar seguimento ao pedido de apagamento dos dados pessoais do interessado e para impedir a divulgação desses dados.

Tendo em conta as considerações precedentes, há que responder à segunda questão que o artigo 17.º do RGPD deve ser interpretado no sentido de que o pedido de um assinante destinado à supressão dos seus dados pessoais das listas constitui um exercício do «direito ao apagamento», na aceção deste artigo.

Quanto à terceira questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 5.º, n.º 2, e o artigo 24.º do RGPD devem ser interpretados no sentido de que uma autoridade de controlo nacional pode exigir que o fornecedor de listas, enquanto responsável pelo tratamento, tome as medidas técnicas e organizacionais adequadas para informar outros responsáveis pelo tratamento, a saber, o operador de serviços telefónicos que lhe comunicou os dados pessoais do seu assinante e os outros fornecedores de listas aos quais ele próprio forneceu esses dados, da retirada do consentimento desse assinante.

A título preliminar, importa salientar que, no caso em apreço, a Proximus tratou dados pessoais do autor da reclamação, publicando-os e comunicando-os a outros fornecedores de listas. A Telenet, o seu operador de serviços telefónicos, tratou igualmente esses dados, nomeadamente transmitindo-os à Proximus. O mesmo se

diga dos outros fornecedores de listas aos quais a Proximus transmitiu os dados de contacto do autor da reclamação e que os publicaram.

Além disso, importa salientar, por um lado, que, como foi recordado no n.º 20 do presente acórdão, embora a Lei Relativa às Comunicações Eletrónicas obrigue os operadores de serviços telefónicos a transmitirem os dados relativos aos seus assinantes aos fornecedores de listas públicas, esses operadores devem, todavia, separar os dados relativos aos assinantes que pediram para não figurar numa lista, de modo a que esses assinantes possam receber uma cópia dessa lista sem que os seus dados nela figurem.

Resulta dos autos de que o Tribunal de Justiça dispõe que, na prática, o consentimento do assinante no sentido de que os seus dados pessoais sejam publicados numa lista é geralmente dado ao seu operador de serviços telefónicos, sendo que tal consentimento permite que esses dados sejam transferidos para um terceiro, fornecedor de listas. Esse fornecedor pode, por sua vez, comunicar esses dados a outros fornecedores de listas, com base no mesmo consentimento, sendo que esses responsáveis pelo tratamento formam uma cadeia, tratando cada um deles sucessivamente os referidos dados, de maneira independente, com base num único e mesmo consentimento.

Resulta igualmente dos autos de que o Tribunal de Justiça dispõe que a atualização da base de dados da Proximus para dar resposta à retirada do consentimento do autor da reclamação foi apagada assim que o seu operador de serviços telefónicos enviou à Proximus uma nova lista de dados relativos aos seus assinantes, para a respetiva publicação nas listas, a qual não tinha em conta a retirada do consentimento do autor da reclamação junto da Proximus.

Neste contexto, coloca-se a questão de saber se um fornecedor de listas, como a Proximus, nos casos em que um assinante de um operador de serviços telefónicos retire o seu consentimento para figurar nas listas desse fornecedor, deve, não só atualizar a sua própria base de dados para ter em conta essa retirada, mas igualmente informar o operador de serviços telefónicos que lhe comunicou esses dados, e os outros fornecedores de listas a que ele próprio transmitiu esses dados, a respeito dessa retirada.

Em primeiro lugar, importa recordar que o artigo 6.º, n.º 1, alínea a), do RGPD prevê que um tratamento é lícito se e na medida em que o titular dos dados

tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas. Ora, resulta da decisão prejudicial que o autor da reclamação retirou o seu consentimento, na aceção do artigo 7.º, n.º 3, deste regulamento, para o tratamento dos seus dados pessoais para fins de publicação em listas. Na sequência dessa retirada, o tratamento desses dados para efeitos da respetiva inscrição nas listas públicas, incluindo o tratamento efetuado com a mesma finalidade por parte dos operadores de serviços telefónicos ou de outros fornecedores de listas que se baseiem no mesmo consentimento, deixa de ter fundamento jurídico e é, assim, ilícito à luz do artigo 6.º, n.º 1, alínea a), do referido regulamento.

Em segundo lugar, importa recordar que, em conformidade com o artigo 5.º, n.º 1, alínea a), e n.º 2, do RGPD, o responsável pelo tratamento deve certificar-se de que está em condições de demonstrar que os dados pessoais são tratados de maneira lícita, leal e transparente em relação ao titular dos dados.

No que respeita ao artigo 24.º do RGPD, este exige que, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, o responsável pelo tratamento aplique as medidas técnicas e organizacionais que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com esse regulamento.

Como salientou o advogado-geral no n.º 67 das suas conclusões, o artigo 5.º, n.º 2, e o artigo 24.º do RGPD impõem obrigações gerais de responsabilidade e cumprimento aos responsáveis pelo tratamento de dados pessoais. Em especial, estas disposições exigem que os responsáveis pelo tratamento adotem as medidas adequadas para prevenir

eventuais violações das regras previstas no RGPD, a fim de assegurar o direito à

proteção de dados.

Nesta perspetiva, o artigo 19.º do RGPD prevê, nomeadamente, que o responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer apagamento de dados pessoais a que se tenha procedido em conformidade com o artigo 17.º, n.º 1, deste regulamento,

salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado.

Ora, decorre das obrigações gerais previstas no artigo 5.º, n.º 2, e no artigo 24.º do RGPD, lidos em conjugação com o seu artigo 19.º, que um responsável pelo tratamento de dados pessoais, como a Proximus, deve aplicar medidas técnicas e organizacionais adequadas para informar os outros fornecedores de listas, aos quais forneceu tais dados, a respeito do facto de a pessoa em causa ter retirado o consentimento que lhe tinha dirigido. Em circunstâncias como as especificadas no n.º 76 do presente acórdão, esse responsável pelo tratamento deve igualmente velar por informar o operador de serviços telefónicos que lhe comunicou esses dados pessoais para que este último adapte a lista dos dados pessoais que transmite automaticamente a esse fornecedor de listas e isole os dados dos seus assinantes que manifestaram a vontade de retirar o seu consentimento para que esses dados fossem tornados públicos.

Com efeito, quando, como no caso em apreço, diferentes responsáveis pelo tratamento se baseiam no consentimento único da pessoa em causa para tratar os seus dados pessoais com a mesma finalidade, basta que, para retirar tal consentimento, essa pessoa se dirija a qualquer um dos responsáveis pelo tratamento, que se baseiam nesse mesmo consentimento, para obter a retirada solicitada.

Como acertadamente salienta a Comissão, para garantir a efetividade do direito de retirar o seu consentimento, previsto no artigo 7.º, n.º 3, do RGPD, e assegurar que o consentimento da pessoa em causa está estritamente ligado à finalidade para a qual o mesmo foi dado, o responsável pelo tratamento, junto do qual a pessoa em causa tenha retirado o seu consentimento para o tratamento dos seus dados pessoais, é efetivamente obrigado a informar dessa retirada qualquer pessoa que lhe tenha transmitido esses dados, bem como a pessoa a quem, por sua vez, esse responsável os tenha transmitido. Os responsáveis pelo tratamento assim informados têm depois, por sua vez, a obrigação de transmitir essas informações aos outros responsáveis pelo tratamento aos quais comunicaram esses dados.

A este respeito, importa, antes de mais, salientar que tal obrigação de informação visa prevenir qualquer violação eventual das regras previstas no RGPD

para assegurar o direito à proteção de dados e, assim sendo, inscreve-se, no âmbito das medidas adequadas, na aceção do artigo 24.º deste regulamento. Além disso, como salientou o advogado-geral no n.º 68 das suas conclusões, inscreve-se igualmente no âmbito da exigência prevista no artigo 12.º, n.º 2, deste regulamento, por força do qual o responsável pelo tratamento é obrigado a facilitar aos titulares de dados o exercício dos seus direitos ao abrigo nomeadamente do artigo 17.º do referido regulamento.

Em seguida, há que constatar que, se o responsável pelo tratamento não estivesse sujeito a tal obrigação de informação da retirada do consentimento da pessoa em causa, essa retirada do consentimento poderia tornar-se particularmente difícil, uma vez que essa pessoa poderia considerar-se obrigada a dirigir-se a cada um dos operadores. Tal abordagem seria, assim, contrária ao artigo 7.º, n.º 3, do RGPD, segundo o qual deve ser tão simples retirar como dar o seu consentimento para o tratamento de dados pessoais.

Por último, em conformidade com a jurisprudência recordada no n.º 49 do presente acórdão, o consentimento, nos termos do artigo 12.º, n.º 2, da Diretiva 2002/58, de um assinante devidamente informado, para a publicação numa lista pública dos seus dados pessoais diz respeito à finalidade dessa publicação e é assim extensivo a qualquer tratamento posterior dos referidos dados por parte de empresas terceiras que operam no mercado das listas, desde que esses tratamentos prossigam essa mesma finalidade.

Daqui resulta que, como salientou o advogado-geral no n.º 68 das suas conclusões, uma vez que o fornecedor de listas pode invocar o consentimento que um assinante tenha dado, para essa finalidade, a outro fornecedor ou ao seu operador de serviços telefónicos, o assinante, para retirar o seu consentimento, deve poder contactar qualquer um dos fornecedores de listas ou o referido operador para retirar os seus dados de contacto das listas publicadas por todos os que se tenham baseado no seu ato único de consentimento.

Tendo em conta as considerações precedentes, há que responder à terceira questão que o artigo 5.º, n.º 2, e o artigo 24.º do RGPD devem ser interpretados no sentido de que uma autoridade de controlo nacional pode exigir que o fornecedor de listas, enquanto responsável pelo tratamento, tome as medidas técnicas e

organizacionais adequadas para informar os terceiros responsáveis pelo tratamento, a saber, o operador de serviços telefónicos que lhe comunicou os dados pessoais do seu assinante e os outros fornecedores de listas aos quais tenha fornecido esses dados, da retirada do consentimento desse assinante.

Com a sua quarta questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 17.º, n.º 2, do RGPD deve ser interpretado no sentido de que se opõe a que uma autoridade de controlo nacional ordene a um fornecedor de listas, ao qual o assinante de um operador de serviços telefónicos pediu que deixasse de publicar os seus dados pessoais, que tome as «medidas que forem razoáveis», na aceção desta disposição, para informar os fornecedores de motores de busca desse pedido de apagamento dos dados.

Para responder a esta questão, importa recordar que o artigo 17.º, n.º 2, do RGPD impõe ao responsável pelo tratamento que tornou públicos os dados pessoais, tendo em conta as tecnologias disponíveis e os custos da sua aplicação, que tome medidas razoáveis, incluindo de ordem técnica, para informar os responsáveis pelo tratamento efetivo desses dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

Como resulta do considerando 66 do RGPD, o objetivo desta obrigação é o reforço do direito a ser esquecido no ambiente por via eletrónica, sendo que, consequentemente, a mesma visa em especial as informações disponibilizadas na Internet pelos fornecedores de motores de busca que tratam dados publicados por via eletrónica.

No caso em apreço, é pacífico que a Proximus publicou, na sua lista, os dados pessoais do autor da reclamação e, portanto, que esta sociedade deve ser considerada um responsável pelo tratamento que tornou públicos esses dados, na aceção do artigo 17.º,

n.º 2, do RGPD.

Além disso, há que recordar que, em conformidade com jurisprudência constante, a atividade de um motor de busca que consiste em encontrar informações publicadas ou disponibilizadas na Internet por terceiros, indexá-las de maneira automática, em armazená-las temporariamente e, por último, em pô-las à

disposição dos internautas segundo uma ordem de preferência determinada, deve ser qualificada de «tratamento» de dados pessoais, na aceção do artigo 4.º, n.º 2, do RGPD, quando essas informações contenham dados pessoais e, por outro lado, que o operador desse motor de busca deve ser considerado «responsável» pelo referido tratamento, na aceção do artigo 4.º, n.º 7, deste regulamento, e, portanto, igualmente do seu artigo 17.º, n.º 2, [v., neste sentido, Acórdão de 24 de setembro de 2019, GC e o. (Supressão de referências e dados sensíveis), C-136/17, EU:C:2019:773, n.º 35 e jurisprudência referida].

Por conseguinte, em circunstâncias como as que estão em causa no processo principal, há que considerar que um responsável pelo tratamento como a Proximus é obrigado, por força do artigo 17.º, n.º 2, do RGPD, a tomar medidas razoáveis para informar os motores de busca do pedido que lhe foi dirigido pelo assinante de um operador de serviços telefónicos com vista ao apagamento dos seus dados pessoais. Todavia, como salientou o advogado-geral no n.º 76 das suas conclusões, para apreciar a razoabilidade das medidas tomadas pelo fornecedor de listas, o artigo 17.º, n.º 2, do RGPD prevê que devem ser tidos em conta a tecnologia disponível e os custos da sua aplicação, tarefa que incumbe principalmente à autoridade competente nesta matéria e que está sujeita a fiscalização jurisdicional.

No caso em apreço, resulta das observações escritas apresentadas pela APD, que não foram contestadas neste ponto pelas outras partes no presente processo, que, no segundo trimestre de 2020, o número de fornecedores de motores de busca que operam na Bélgica era limitado. Em particular, a Google detinha uma quota de mercado compreendida entre 90 %, no que respeita às pesquisas em computadores fixos, e 99 %, no que respeita às pesquisas em *smartphones* e *tablets*.

Além disso, como foi indicado no n.º 26 do presente acórdão, resulta dos autos submetidos ao Tribunal de Justiça que, na sequência do pedido do assinante para que os seus dados não fossem incluídos nas listas desse fornecedor, a Proximus respondeu que não só tinha suprimido esses dados das listas telefónicas e dos serviços de informação telefónica, como também tinha contactado a Google para que as hiperligações pertinentes para o sítio Internet da Proximus fossem suprimidas.

Tendo em conta as considerações precedentes, há que responder à quarta questão que o artigo 17.º, n.º 2, do RGPD deve ser interpretado no sentido de que

não se opõe a que uma autoridade de controlo nacional ordene a um fornecedor de listas, ao qual o assinante de um operador de serviços telefónicos pediu que deixasse de publicar os seus dados pessoais, que tome as «medidas que forem razoáveis», na aceção desta disposição, para informar os fornecedores de motores de busca desse pedido de apagamento dos dados.

Pelos fundamentos expostos, o Tribunal de Justiça (Quarta Secção) declarou que o artigo 12.º, n.º 2, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido em conjugação com o artigo 2.º, segundo parágrafo, alínea f), desta diretiva e o artigo 95.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), deve ser interpretado no sentido de que: é exigido o «consentimento», na aceção do artigo 4.º, ponto 11, desse regulamento, do assinante de um operador de serviços telefónicos para que os dados pessoais desse assinante figurem nas listas e nos serviços de informação telefónica públicos, publicados por fornecedores diferentes desse operador, podendo esse consentimento ser dado quer ao referido operador quer a um dos seus fornecedores.

O artigo 17.º do Regulamento 2016/679 deve ser interpretado no sentido de que o pedido de um assinante destinado à supressão dos seus dados pessoais das listas e dos serviços de informação telefónica públicos constitui um exercício do «direito ao apagamento», na aceção deste artigo.

O artigo 5.º, n.º 2, e o artigo 24.º do Regulamento 2016/679 devem ser interpretados no sentido de que uma autoridade de controlo nacional pode exigir que o fornecedor de listas e de serviços de informação telefónica públicos, enquanto responsável pelo tratamento, tome as medidas técnicas e organizacionais adequadas para informar os terceiros responsáveis pelo tratamento, a saber, o operador de serviços telefónicos que lhe comunicou os dados pessoais do seu assinante e os outros fornecedores de listas e de serviços de informação telefónica

públicos aos quais tenha fornecido esses dados, da retirada do consentimento desse assinante.

O artigo 17.º, n.º 2, do Regulamento 2016/679 deve ser interpretado no sentido de que não se opõe a que uma autoridade de controlo nacional ordene a um fornecedor de listas e de serviços de informação telefónica públicos, ao qual o assinante de um operador de serviços telefónicos pediu que deixasse de publicar os seus dados pessoais, que tome as «medidas que forem razoáveis», na aceção desta disposição, para informar os fornecedores de motores de busca desse pedido de apagamento dos dados.

Conclusão

A escolha do acórdão em análise teve como objetivo verificarmos como é tratada a questão da proteção de dados no âmbito das comunicações eletrónicas à luz do RGPD, sendo que, independentemente de não se tratar de uma empresa portuguesa, estamos perante um caso da União, criando -se assim jurisprudência.

Ora, e a Jurisprudência que mais nos ressaltou foi a questão do consentimento no âmbito das comunicações eletrónicas. Aliás, quando pensamos neste tema, era nosso objetivo entendermos, como se equaciona e como se protege situações de tratamento de dados pessoais perante as novas tecnologias que hoje ultrapassam fronteiras numa velocidade tão rápida.

E pelo que vimos neste acórdão, o Regulamento (UE) 2016/679, numa versão muito mais atual e com normas mais exequíveis, não permite deixar passar situações como a que, a título exemplificativo, vimo no acórdão.

Recordemos -nos que à páginas **6 a 14** fiz questão de colocar a definição de vários conceitos / definições constantes da nossa Lei interna que é a Lei n.º 16/2022 de 16 de Agosto. A situação aplica -se nos mesmos termos, ou seja, não é possível colocar a pessoa singular na posição de, por exemplo, consumidor, se não houver esta solicitação da parte da própria pessoa, sendo que tem que haver aqui a liberdade da mesma, claro que respeitando o contrato que assinou, de rescindi – lo

e de não querer ver os seus dados a serem continuados a serem tratados pela entidade que prestava o serviço de comunicação eletrónica.

No caso em concreto, estamos perante uma decisão do Tribunal de Justiça da União Europeia que respeitou os princípio da licitude e transparência (art.º 5/1 al a, 6.º do RGPD) e os direitos ao apagamento dos dados (direito a ser esquecido) e retificação (art.º 17 e 16 do RGPD, respetivamente), sendo que tudo teve como base o conceito de " consentimento" (art.º 7 e 8.º do RGPD). Conseguimos assim verificar que este consentimento não é aplica apenas à publicação dos dados pessoais, é muito mais abrangente, destacando -se aqui a função da Autoridade de Controlo Nacional.

No nosso país não é diferente: a CNPD assume um papel de extrema importância, emitindo pareceres inclusive aquando de propostas de leis, precisamente na sua posição de Fiscalizador da proteção de dados pessoais. Para além disso, reparemos que embora exista uma autoridade que regule o mercado das comunicações eletrónicas (ANACOM), a mesma deve sempre trabalhar tendo em atenção o RGPD – o art.º 31 da RGPD é claro quanto à necessidade de cooperação com a autoridade de controlo na prossecução das suas atribuições. Aliás, segundo o Professor Menezes Cordeiro, " a atribuição de competências a uma única autoridade de controlo sempre que o tratamento de dados possa ser reconduzido ao conceito de tratamento transfronteiriço, apresenta -se como uma das grandes novidades do RGPD[28]", já que até então vigorava o modelo de "*one stop shop*": o tratamento de dados pessoais ocorria no contexto das atividades de um responsável pelo tratamento ou de um subcontratante estabelecido na união e o responsável pelo tratamento ou o subcontratante que estivesse estabelecido em vários Estados – Membros, a autoridade de controlo onde se situasse o estabelecimento principal do responsável pelo tratamento ou do subcontratante é que era competente para controlar as atividades de tratamento do responsável pelo tratamento ou do subcontratante em todos os Estados – Membros[29].É pertinente realçarmos que as questões resolvidas pelo Tribunal de Justiça da União Europeia foram decisões prejudiciais - Reenvio Prejudicial - , diferente da decisão de mérito que será decidida pelo Tribunal competente – o que procedeu ao reenvio do processo. Porém, também é importante realçar que estando resolvida a questão prejudicial, a decisão de mérito é muito mais fácil de ser decretada e publicada. Para nós, a aplicação de coimas e sanções constante dos artigos 83º e 84 do RGPD,

respetivamente, e 178 (contraordenações e coimas), 179 (Sanções acessórias) e183.º (sanções pecuniárias compulsórias) da Lei n.º 16/2022 de 16 de Agosto para além de ser uma forma de punição dos Estados – Membros, serve de alerta para a importância de um direito fundamental que estava a ser descurado até por cada um de nós. Que haja maior consciência nas nossas ações, pois, como vimos, as consequências são gravosas, até mesmo em situações acidentais.

Referências Bibliográficas

A. Barreto Menezes Cordeiro, "Direito da Proteção de Dados" à Luz do RGPD e da Lei n.º 58/2019, Almedina.

Acórdão do Tribunal de Justiça (Quarta Secção) 27 de outubro de 2022 (*) – Proc. n.º C- 129/21.

Constituição da República Portuguesa.

JORNAL OFICIAL DA UNIÃO EUROPEIA (JOUE)

- Diretivas 98/84/CE do Parlamento Europeu e do Conselho, de 20 de Novembro de 1998, relativa à proteção jurídica dos serviços que se baseiem ou consistam num acesso condicional.

- Diretivas 2002/77/CE da Comissão de 16 de Setembro de 2002, relativa à concorrência nos mercados de redes e serviços de comunicações eletrónicas.(UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de Dezembro de 201 8, que estabelece o Código Europeu das Comunicações eletrónicas.

- Diretivas 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Parecer da CNPD 2021/53 relativo à alterações à Lei da Privacidade nas comunicações Eletrónicas.

Lei 16/2022 de 16 de Agosto – aprova a Lei das Comunicações Eletrónicas, transpondo as Diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972, alterando as Leis n.ºs 41/2004, de 18 de Agosto, e 99/2009, de 4 de Setembro, e os Decretos – Leis n.ºs 151 – A/2000, de 20 de Julho, e 24/2014, de 14 de Fevereiro, e revogando a Lei n.º 5/2004, de 10 de Fevereiro, e a Portaria n.º 791/98, de 22 de Setembro.

Lei n.º 58/2019 de 8 de agosto - assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoas e à livre circulação desses dados.

Inteligência Artificial, Proteção de Dados Sensíveis e a Vulnerabilidade Humana: o plano legal e o plano da bioética

Cristina Maria de Gouveia Caldeira[164]

Resumo

O estudo centra-se numa reflexão sobre a transformação digital da sociedade e os debates ocorridos, sobretudo em 2023, em torno do impacto da aplicação da inteligência artificial (IA) em especial na área da saúde. Trata-se de uma tecnologia emergente, caracterizada pela polivalência, que alcançou maior visibilidade a partir de 2016, numa altura em que a União Europeia desenhava a sua estratégia sobre a IA, a que se seguiu um pacote legislativo em torno da proteção de dados pessoais (RGPD), o qual consagra um regime reforçado de proteção ao tratamento de dados sensíveis. Posteriormente foi criado o *Artificial Intelligence Act*, um quadro regulamentar baseado no risco e publicadas as regras aplicadas à responsabilidade civil extracontratual à inteligência artificial, bem como o Regulamento relativo à Governação Europeia dos Dados. Em ordem ao título: *Inteligência Artificial, Proteção de Dados Sensíveis e a Vulnerabilidade Humana: o plano legal e o plano da bioética* elencamos os seguintes pontos: Sistemas de IA baseados nos valores da União; Transformação dos municípios através da aplicação da IA na área da saúde; Regras específicas relativas aos sistemas de IA aplicados à área da saúde; Privacidade e confidencialidade dos dados sensíveis em contexto multinível; Princípios éticos aplicáveis à prática clínica e investigação médica; Integridade da investigação versus confidencialidade da informação clínica; Bioética e o princípio da autonomia: o consentimento informado; Vulnerabilidade como um conceito ético-jurídico e Governação Europeia de Dados.

Palavras-chave: Dignidade humana, inteligência artificial, dados relativos à saúde, privacidade, proteção de dados sensíveis, vulnerabilidade, bioética.

[164] Jurista, Professora Auxiliar da Universidade Europeia, Investigadora FCT.I.P., Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College.

Artificial Intelligence, Protection Of Sensitive Data and Human Vulnerability: the legal plan and the bioethics plan

Abstract

The study focuses on a reflection on the digital transformation of society and the debates taking place, especially in 2023, around the impact of the application of artificial intelligence (AI), especially in the area of health. It is an emerging technology, characterized by versatility, which achieved greater visibility from 2016 onwards, at a time when the European Union was designing its strategy on AI, which was followed by a legislative package around the protection of personal data. (GDPR), which enshrines a reinforced protection regime for the processing of sensitive data. Subsequently, the Artificial Intelligence Act, a risk-based regulatory framework, was created and the rules applied to non-contractual civil liability for artificial intelligence were published, as well as the Regulation on European Data Governance. In order of the title: Artificial Intelligence, Sensitive Data Protection and Human Vulnerability: the legal plan and the bioethics plan, we list the following points: AI systems based on the values of the Union; Transformation of municipalities through the application of AI in the health sector; Specific rules relating to AI systems applied to the healthcare sector; Privacy and confidentiality of sensitive data in a multilevel context; Ethical principles applicable to clinical practice and medical research; Research integrity versus confidentiality of clinical information; Bioethics and the principle of autonomy: informed consent; Vulnerability as a legal ethical concept and European Data Governance.

Keywords: Human dignity, artificial intelligence, health data, privacy, sensitive data protection, vulnerability, bioethics

Introdução

A intensificação dos debates em torno dos impactos da IA e a discriminação algorítmica, marcaram o ano de 2023. Na mensagem do Dia Mundial da Paz, a 1 de janeiro de 2024, o Santo Padre Francisco realça que,

> "Os progressos da informática e o desenvolvimento das tecnologias digitais, nas últimas décadas, começaram já a produzir profundas transformações na sociedade global e nas suas dinâmicas. Os novos instrumentos digitais estão a mudar a fisionomia das comunicações, da administração pública, da instrução, do consumo, dos intercâmbios pessoais e de inúmeros outros aspetos da vida diária. Além disso as tecnologias que se servem duma multiplicidade de algoritmos podem, dos vestígios digitais deixados na internet, extrair dados que permitem controlar os hábitos mentais e relacionais das pessoas para fins comerciais ou políticos, muitas vezes sem o seu conhecimento, limitando o exercício consciente da sua liberdade de escolha."

Trata-se de uma tecnologia emergente, caracterizada pela polivalência, que alcançou maior visibilidade a partir de 2016, altura em que a presidência japonesa do G7, colocou a IA na agenda, destacando as suas implicações e a necessidade de se garantir a proteção dos dados e a informação pessoal. Por essa altura, a União Europeia desenhava a sua estratégia sobre a IA, a que se seguiu um pacote legislativo em torno da proteção de dados pessoais, consagrando um regime reforçado de proteção ao tratamento de dados sensíveis, onde se incluem os dados relativos à saúde, das regras harmonizadas dos sistemas de IA e da responsabilidade civil da IA, bem como da governação europeia dos dados, numa tentativa de manter a vanguarda do percurso tecnológico mundial ancorado num quadro ético e jurídico robusto, centrado no ser humano e na garantia dos direitos fundamentais.

O Santo Padre Francisco recorda-nos ainda que «a inteligência artificial deve ser entendida como uma galáxia de realidades diversas e não podemos presumir *a priori* que o seu desenvolvimento traga um contributo benéfico para o futuro da humanidade e para a paz entre os povos. O resultado positivo só será possível se nos demonstrarmos capazes de agir de maneira responsável e respeitar valores humanos fundamentais como "a inclusão, a transparência, a segurança, a equidade, a privacidade e a fiabilidade"»[165].

[165] FRANCISCO. Mensagem do Santo Padre para a celebração do Dia Mundial da Paz, 1 de janeiro de 2024.

Por fim, torna-se obrigatória uma reflexão mais adensada sobre a vulnerabilidade humana face à aplicação de tecnologias computacionais inteligentes na saúde e à criação de prestadores de serviços de intermediação de dados, através da entrada em vigor do Regulamento da Governação Europeia de Dados, a 24 de setembro de 2023.

1. Sistemas de inteligência artificial baseados nos valores da União

Em 21 de abril de 2021, a Comissão Europeia publicou uma proposta de regulamento do Parlamento Europeu e do Conselho que veio estabelecer as regras harmonizadas em matéria de inteligência artificial[166]. Trata-se de um enquadramento jurídico dos sistemas de IA, baseado nos valores da União, consagrados na Carta dos Direitos Fundamentais da União Europeia (CDFUE), bem como na Convenção Europeia dos Direitos do Homem (CEDH).

Sob a Presidência espanhola do Conselho da União, no início de dezembro de 2023, o Conselho e o Parlamento chegaram a um acordo, ainda que provisório, sobre a proposta de regras harmonizadas em matéria de IA, apresentadas pela Comissão. O projeto de regulamento, que sofreu alterações face à proposta inicial, pretende garantir que os sistemas de IA colocados no mercado europeu e utilizados na União Europeia, não só ofereçam segurança e respeitem os direitos fundamentais e os valores da União, como também, estimulem o investimento e a inovação na Europa.

Os trabalhos técnicos continuam tendo o texto de regulamento de ser apresentado ao *Coreper* (comité dos representantes dos Estados-Membros) para aprovação e, posteriormente confirmado e submetido à revisão jurídico-linguísticos, antes da adoção formal em 2024. O acordo provisório prevê uma *vacatio legis* de dois anos entre a publicação do diploma no Jornal Oficial da União Europeia e a sua entrada em vigor.

Fora do Regulamento Inteligência Artificial ficou a legislação relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade Civil da IA)[167]. Também nesta matéria foi

[166] JOUE. Regulamento Inteligência Artificial. COM (2021) 206 final.

[167] JOUE. Diretiva Responsabilidade da IA. COM (2022) 496 final.

alcançado, no dia 14 de dezembro de 2023, um acordo político entre os Estados-Membros. Juntamente com o Regulamento Inteligência Artificial, a Diretiva Responsabilidade Civil da IA faz parte de um pacote de medidas destinadas a apoiar a implantação da IA na Europa mediante a promoção da excelência e da confiança. E, em virtude da inadequação das atuais regras nacionais de responsabilidade, em especial em matéria de responsabilidade culposa, ao tratamento de ações de indemnização por danos causados por produtos e serviços assentes em IA, a presente proposta oferece, às vítimas de danos causados pela IA, uma proteção equivalente à das vítimas de danos causados por produtos em geral, evitando a fragmentação das regras nacionais de responsabilidade civil específicas para a IA.

Inteligência Artificial é uma família de técnicas de programação informática extremamente poderosas, que não obstante as inúmeras vantagens da sua aplicação, as características específicas de determinados sistemas de IA (incluindo a complexidade, a autonomia e a opacidade, o denominado efeito de "caixa negra") podem criar novos riscos relacionados com a segurança e a proteção, pôr em causa a vida privada e familiar, bem como a proteção dos dados pessoais, direitos fundamentais consagrados na CDFUE, bem como acelerar a probabilidade ou intensidade dos riscos existentes.

As Nações Unidas publicaram, em dezembro de 2023, o Relatório provisório: *Governing AI for Humanity*[168], que lança uma proposta para a governação internacional da IA, baseada na Carta das Nações Unidas e no seu compromisso para a paz, a segurança, os direitos humanos e o desenvolvimento sustentável, bem como na legislação internacional sobre Direitos Humanos. Nessa conformidade, deverá avaliar-se regularmente o estado da IA e a sua trajetória, harmonizar padrões, segurança e gestão de riscos, promover a colaboração multissetorial internacional, monitorar riscos e coordenar a resposta a emergências e desenvolver normas vinculativas de responsabilização.

Wolfgang Hoffmann-Riem, na sua obra Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito, oferece-nos uma visão científica dos principais temas relacionados com o fenómeno da digitalização, bem como noções sólidas de algoritmos, IA e "big data". Com grande atualidade e pertinência, o autor

[168] NAÇÕES UNIDAS. *Interim Report: Governing AI for Humanity*, *AI* Advisory Body, dezembro 2023.

aborda as regras técnicas, legais e sociais, contidas nos algoritmos digitais. Refere que os algoritmos são indispensáveis em quase todas as áreas da sociedade sendo, no entanto, uma descoberta problemática, pelos riscos que representa designadamente na manipulação de comportamentos e nas ameaças à privacidade[169].

Graças à convergência de fatores como o aumento da capacidade computacional, a multiplicação dos conjuntos de dados e a evolução dos algoritmos[170], a IA entrou numa nova era, transformando-se numa das áreas de investigação científica multidisciplinar mais complexas, atual e promissora. Esses progressos da ciência e da tecnologia oferecem grandes benefícios à humanidade, nomeadamente aumentando a esperança de vida e melhorando a qualidade de vida. Porém, estes avanços devem ser guiados pela dignidade da pessoa humana e pelo respeito universal e efetivo dos direitos humanos e das liberdades fundamentais.

Conscientes da transformação digital da sociedade, assumimos a relevância de incluir neste estudo, o setor da saúde, por se encontrar numa fase de grande carência, em toda a Europa. É comumente aceite que, face a uma população envelhecida e carenciada de serviços de saúde, não haverá profissionais de saúde suficientes para prestar os serviços que a população necessita. Mas, a aplicação das novas tecnologias (IA e robótica) no setor da saúde é altamente promissora. E, a confluência entre a revolução digital e a revolução genómica, abre as portas à inovação na área da saúde. Vivemos um momento de esperança!

Ainda assim, reconhecendo que a saúde não depende apenas dos progressos da investigação científica e tecnológica, mas também de fatores psicossociais e culturais, e que as decisões relativas às questões éticas suscitadas pela medicina, pelas ciências da vida e pelas tecnologias que lhes estão associadas, podem ter repercussões sobre a humanidade em geral, procura-se contextualizar a forte transformação digital da saúde, de que resulta uma forte procura de soluções

[169] HOFFMANN-REIM, WOLFGANG. Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito, p. 11-13.

[170] PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial.

tendo por base a bioética, bem como a problematização das soluções de equidade.

Os riscos para a privacidade dos titulares dos dados de saúde são elevados. Desse modo, ao aplicar todo o potencial tecnológico em áreas como "a telessaúde, a cirurgia robótica, o seguimento dos doentes via *wearables* ou a implementação de modelos primitivos para a decisão clínica, a segurança e a privacidade dos dados são primordiais"[171].

O novo contexto traz obrigatoriamente ao debate os desafios éticos da transformação digital, a proibição do tratamento de categorias especiais de dados pessoais, tal como prevê o n.º 1 do Art.º 9.º do Regulamento (UE) 2016/679, de 27 de abril - Regulamento Geral de Proteção de Dados (RGPD)[172], bem como uma reflexão sobre a vulnerabilidade, conceito por muito tempo arredado do Direito, mas que defendemos neste estudo (trata-se de um conceito ético-jurídico, com grande contribuição da Bioética). Neste plano, importa recordar as palavras do Santo Padre Francisco, que recentemente nos alertava para a necessidade de serem criados modelos normativos, que ofereçam uma orientação ética aos criadores de tecnologias digitais. Nas suas palavras, o Santo Padre refere que

> "é indispensável identificar os valores humanos que deveriam estar na base dos esforços das sociedades para formular, adotar e aplicar os quadros legislativos necessários. O trabalho de elaboração de diretrizes éticas para a produção de formas de inteligência artificial não pode prescindir da consideração de questões mais profundas relativas ao significado da existência humana, à proteção dos direitos humanos fundamentais, à busca da justiça e da paz. Este processo de discernimento ético e jurídico pode revelar-se preciosa ocasião para uma reflexão compartilhada sobre o papel que a tecnologia deveria ter na nossa vida individual e comunitária e sobre a forma como a sua utilização possa contribuir para a criação dum mundo mais equitativo e humano. Por este motivo, nos debates sobre a regulamentação da inteligência artificial, dever-se-ia ter em conta as vozes de todas as partes interessadas, incluindo os pobres, os marginalizados e outros que muitas vezes permanecem ignorados nos processos de decisão globais."[173]

[171] VITORINO, G; CORDEIRO, J.; MAGALHÃES, T., A transformação digital nas suas diversas dimensões, *apud* Transformação digital em Saúde (2021).

[172] JOUE. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[173] FRANCISCO. Mensagem do Santo Padre para a celebração do Dia Mundial da Paz, 1 de janeiro de 2024.

Na perspetiva defendida no presente estudo, a aplicação das novas tecnologias nos vários domínios da nossa vida deve assentar no princípio da dignidade da pessoa humana, princípio estruturante que se constitui como um farol, um fundamento ético-jurídico, um valor subjacente aos direitos fundamentais e reciprocamente influenciado pela autonomia pessoal, um princípio bioético que se traduz pela defesa da autodeterminação de cada pessoa em tomar decisões em relação à sua vida e em concreto, à saúde.

Concretizando o contributo da bioética para a autodeterminação da pessoa portadora de doença, encontra-se presente, quer nos códigos deontológicos dos profissionais de saúde, quer nos instrumentos internacionais, como é exemplo a Convenção para a Protecção dos Direitos do Homem e da Dignidade do ser Humano face às aplicações da Biologia e da Medicina: Convenção sobre os Direitos do Homem e a Biomedicina.

2. Transformação dos municípios através da aplicação da IA na área da saúde

Tendo presente a tendência atual de uma população cada vez mais envelhecida, já anteriormente brevemente aflorada, assume-se como relevante a Estratégia Nacional de Territórios Inteligentes (ENTI), aprovada pela Resolução do Conselho de Ministros n.º 176/2023, de 18 de dezembro, juntamente com o seu Plano de Ação e a Arquitetura de Referência para Plataformas de Gestão Urbana (ARPGU)[174].

Os instrumentos acima referidos mobilizam a atuação dos municípios em torno da oferta de cuidados de saúde. Porém, a "evolução de um ecossistema de territórios inteligentes para um ecossistema nacional inteligente", irá requer:

> "um processo de transformação nacional que inclui as áreas urbanas e não-urbanas, exigindo uma forte cooperação entre todos os atores relevantes, um alinhamento entre os interesses e prioridades nacionais, do setor público, empresas e sociedade e, uma integração e interoperabilidade entre os territórios de forma a criar valor e melhorar a qualidade de vida das pessoas. A contribuir para essa evolução estarão as tecnologias emergentes, tais como o 5G, *internet of things* (IoT), *cloud, edge computing*, realidade aumentada e virtual,

[174] Agência para a Modernização Administrativa (AMA). Estratégia Nacional de Territórios Inteligentes-ENTI (2023-2030), 2023.

> inteligência artificial (IA), gémeos digitais, multiverso e analítica avançada, que irão amplificar o impulso estratégico de transformação dos territórios." (ENTI, p. 10,11)

A evolução de um ecossistema de territórios inteligentes assenta na utilização da IA aplicada a um conjunto de serviços públicos locais. A aplicação algorítmica irá exigir a agregação de dados em plataformas integradas, bem como a interoperabilidade desses mesmo dados. Nessa medida, quando em causa estejam dados pessoais e em especial dados pessoais sensíveis (dados de saúde e outros dados pessoais relativos às condições socioeconómicas das populações), serão consideradas operações de um risco elevado no âmbito do Regulamento Inteligência Artificial. Em face dos riscos associados à evolução pretendida, assume-se como necessário um grande investimento ao nível da arquitetura da infraestrutura tecnológica, de modo a cumprir as obrigações que resultam do referido regulamento. Segundo a ENTI

> "O 5G pode e deve acelerar a coesão territorial através de uma Administração Pública mais próxima, que disponibiliza serviços públicos com soluções e canais adaptados às circunstâncias locais. Através da conjugação da possibilidade de medição em IoT, da capacidade de análise e tratamento avançado de dados, e da integração de modelos IA para extração de conhecimento, alavancadas na transmissão massiva de informação e em tempo real (5G). (…) Esta dimensão tecnológica inclui a agregação de dados e dos processos associados (recolha, tratamento, armazenamento, utilização e partilha) em plataformas integradas, garantindo a interoperabilidade dos vários sistemas relevantes neste contexto, através de interfaces de programação de aplicação (APIs)[175] e serviços de integração." (ENTI, p. 11)

Relevante é o conjunto de Recomendações que a ENTI prevê e que devem integrar os planos locais, podendo a sua aplicação ser ajustada pelo Município e/ou Comunidades Intermunicipais/Áreas Metropolitanas (CIMs/AMs), consoante a maturidade que apresente. Entre os domínios mais relevantes em matéria de tratamento de dados relativos à saúde, sinalizamos os seguintes:

(i) Sociedade inteligente, cuja recomendação consiste em: "Promover atividades de promoção da **saúde** e de inclusão social, de forma a promover a adoção de estilos de vida saudáveis e a prevenção de comportamentos de risco,

[175] Application Programming Interfaces (APIs)

assim como a requalificação de pessoas socialmente excluídas e ações no âmbito da rede de apoio social."

(ii) Qualidade de vida inteligente, que recomenda a adoção de: "Implementar parcerias entre municípios e entidades de **saúde,** em alinhamento com o Plano Nacional de Saúde 2030 e os Planos Locais de Saúde, contribuindo para a melhoria da saúde das populações e o reforço da acessibilidade, eficiência e diferenciação da oferta de cuidados de saúde de proximidade (telessaúde, teleassistência)" (ENTI, p. 18, 19)

Além da área da saúde, a ENTI consagra outras iniciativas com recurso à IA, igualmente promissoras, e, tendo a aplicação do Regulamento Inteligência Artificial o propósito de garantir que os diferentes sistemas de IA colocados no mercado europeu, ofereçam segurança e respeitem os direitos fundamentais, a IA passará a ser regulamentada com base na sua capacidade para causar danos à sociedade. Trata-se de um enquadramento legal baseado no risco, que estabelece a diferença entre as utilizações que criam um risco inaceitável, um risco elevado e um risco baixo ou mínimo.

Em defesa dos direitos fundamentais e dos valores da União, o Título II da proposta de Regulamento IA, consagra as práticas que determinam um risco inaceitável, ou seja, a aplicação dos sistemas IA proibidos[176]. As proibições, que foram expandidas no acordo provisório alcançado em dezembro de 2023, entre o Parlamento e o Conselho, prendem-se com práticas que visam manipular as pessoas, por meio de técnicas subliminares, sem que estas se apercebam, ou exploram as vulnerabilidades de grupos específicos, como as crianças ou as pessoas com deficiência, levando à alteração dos seus comportamentos de uma forma que seja suscetível de causar a si, ou a outra pessoa, danos psicológicos ou físicos[177].

Para além do alargamento das práticas de IA proibidas, o acordo provisório reafirma as regras aplicáveis aos modelos de IA de finalidade geral e de grande impacto, que possam representar um risco sistémico no futuro, bem como os sistemas de inteligência artificial de risco elevado (Título III) para a saúde, segurança e direitos fundamentais das pessoas, designadamente os sistemas utilizados na gestão do tráfego rodoviário, no recrutamento ou seleção de pessoas, entre outros. Nestes

[176] *Idem*, artigo 5.º.

[177] JOUE. COM (2021)206 final, p. 14.

casos estão previstos requisitos apertados dirigidos a estes sistemas de IA, impondo-se a necessidade de implementação de um sistema de gestão do risco e a obrigatoriedade de realização de uma avaliação de impacto sobre os direitos fundamentais, antes dos sistemas de IA serem colocados no mercado.

Por último, os fornecedores de sistemas de inteligência artificial classificados de baixo risco poderão aderir voluntariamente ao cumprimento dos requisitos estabelecidos na Proposta de Regulamento, através da criação e implementação dos seus próprios códigos de conduta, podendo incluir compromissos voluntários de sustentabilidade ambiental, tal como se prevê no Título IX.

Foi ainda revisto o sistema de governação, que é um dos quatro objetivos constantes da Proposta (Título VI), no sentido de introduzir poderes de execução de forma a melhorar a governação e a aplicação do Regulamento e demais legislação em vigor em matéria de direitos fundamentais, bem como os requisitos de segurança aplicáveis aos sistemas de IA.

Do exposto, sublinha-se, que o quadro jurídico da IA será aplicável aos programas informáticos que permitem a aprendizagem automática, às abordagens baseadas na programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais, bem como abordagens estatísticas[178]. Importa ainda ter presente, que estão previstas regras e novas obrigações, num âmbito de uma aplicação alargada, que inclui a maioria dos intervenientes na cadeia de produção de IA, como fornecedores de IA, entidades que utilizam sistemas de IA, importadores, distribuidores, fabricantes de produto e representantes autorizados.

Apelidada de "emblemática", a iniciativa legislativa que deverá ser publicada em 2024, tem o potencial de promover o desenvolvimento e a adoção de uma IA segura e fiável na União, por entidades públicas e privadas. Atendendo ao seu âmbito, o Regulamento Inteligência Artificial será aplicável às entidades,

[178] *Vide* (Anexo I, Técnicas e Abordagens no domínio da IA, referidas no artigo 3.º, ponto 1) a) Abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda; b) Abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais; c) Abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização.) Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_2&format=PDF

mesmo que não se encontrem estabelecidas na União Europeia, sendo apenas necessário que o sistema de IA seja colocado no mercado ou ao serviço do mercado europeu, ou ainda que o resultado produzido pelo sistema de IA seja utilizado na União Europeia[179].

3. Regras específicas relativas aos sistemas de IA aplicados à área da saúde

Vimos anteriormente que o Regulamento Inteligência Artificial consagra, no Título III da Proposta, as regras específicas relativas aos sistemas de IA que criam um risco elevado para a saúde e a segurança ou para os direitos fundamentais de pessoas singulares.

A classificação de um sistema de IA como de risco elevado tem por base a finalidade para a qual foi criado o programa informático, em conformidade com a atual legislação relativa à segurança de produtos. Estes sistemas continuarão a ser autorizados no mercado europeu, mas sujeitam-se ao cumprimento de determinados requisitos obrigatórios e a uma avaliação da conformidade "ex ante", em clara complementaridade com o RGPD.

Tomando por exemplo o *Digital Tracking and Tracing System* (DTTS), um sistema aparentemente criado para rastrear a propagação da COVID-19, foi altamente escortinado pelas Autoridades Nacionais de Proteção de Dados na Europa, tendo sido exigida uma apurada avaliação de impacto de proteção de dados "ex ante", em conformidade com o Art.º 35.º do RGPD.

O RGPD dispõe sobre os dados relativos à saúde no n.º 1 do Art.º 9.º, protegendo estes dados de uma forma especial por se tratar de categorias especiais de dados pessoais. Nessa categoria incluem-se as informações sobre a pessoa singular, recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, bem como qualquer número, símbolo ou sinal particular que lhe seja atribuído, a fim de a identificar de forma inequívoca para fins de cuidados de saúde. Integram-se ainda nesta categoria, as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a informação recolhida a partir de dados genéticos e amostras biológicas, bem como qualquer informação relativa a uma doença, deficiência, risco de doença,

[179] JOUE. COM (2021)206 final, alínea c) do n.º 1 do artigo 2.º.

historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte (médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*). Em todos os exemplos acima citados estamos a tratar dados pessoais sensíveis.

Um sistema de IA com a finalidade específica de tratamento dos dados sensíveis poderá materializar um risco elevado para uma pessoa concretamente identificada ou identificável, caso sejam incumpridos os requisitos legais relativamente aos dados e à governação de dados, à documentação e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à segurança, tal como se encontram previstos no Capítulo 2 do Titulo III da Proposta do Regulamento Inteligência Artificial.

Não obstante os desafios identificados, defendemos que a transformação digital dos serviços de saúde apresenta-se muito promissora. A esse propósito, recordemos o excelente trabalho do Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial (GPAN IA)[180], que em 2019, apresentou as Orientações éticas para uma inteligência artificial. Nesse documento, deu a conhecer vários projetos na área da saúde e do bem-estar, tais como: Projeto MURAB (*MRI and Ultrasound Robotic Assisted Biopsy*); Projeto REVOLVER (*Repeated Evolution of Cancer*); Projeto LIVE INCITE; Projeto CARESSES (*Culture-Aware Robots and Environmental Sensor Systems for Elderly Support*); cujo tratamento inteligente foram determinantes para a prevenção de doenças potencialmente mortais.

Em suma, conscientes dos riscos para a confidencialidade, disponibilidade e integridade dos dados sensíveis associados à transformação digital na área da saúde, sublinhamos a relevância dos instrumentos jurídicos europeus referidos, em defesa dos direitos fundamentais e dos valores da União. Porém, dogmaticamente o tema da proteção de dados pessoais relativos à saúde obriga-nos a uma reflexão em contexto de regulação de múltiplos níveis, de construção e execução de instrumentos jurídicos europeus e internacionais. A esse propósito, voltamos ao Relatório provisório das Nações Unidas: *Governing AI for Humanity*[181], e em concreto,

[180] Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial, *Orientações éticas para uma inteligência artificial*, p. 14.

[181] NAÇÕES UNIDAS. *Interim Report: Governing AI for Humanity*, *AI* Advisory Body, dezembro 2023.

ao lançamento de uma proposta para a governação internacional da IA baseada na Carta das Nações Unidas e na legislação internacional sobre Direitos Humanos, o que nos leva a questionar se será possível a criação de uma norma mundial para a aplicação da IA na área da saúde.

4. Privacidade e confidencialidade dos dados sensíveis em contexto multinível

A privacidade e a confidencialidade dos dados sensíveis, onde se incluem os dados de saúde e os dados genéticos, encontram consagração no n.º 1 do Art.º 9.º do RGPD, e em outros instrumentos jurídicos internacionais, designadamente na Declaração Internacional sobre os Dados Genéticos Humanos, adotada pela Conferência Geral da UNESCO em 16 de outubro de 2003[182], que no seu Art.º 14.º alínea b) refere, que

> "Os dados genéticos humanos[183], os dados proteómicos humanos[184] e as amostras biológicas[185] associados a uma pessoa identificável não deverão ser comunicados nem tornados acessíveis a terceiros, em particular empregadores, companhias de seguros, estabelecimentos de ensino ou família, se não for por um motivo de interesse público importante nos casos restritivamente previstos pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos, ou ainda sob reserva de consentimento prévio, livre, informado e expresso da pessoa em causa, na condição de tal consentimento estar em conformidade com o direito interno e com o direito internacional relativo aos direitos humanos. A vida privada de um indivíduo que participa num estudo em que são utilizados dados genéticos humanos, dados proteómicos humanos ou amostras biológicas deverá ser protegida e os dados tratados como confidenciais."

[182] Declaração Internacional sobre os Dados Genéticos Humanos, 16 de outubro de 2003.

[183] Dados genéticos humanos: informações relativas às características hereditárias dos indivíduos, obtidas pela análise de ácidos nucleicos ou por outras análises científicas; [Declaração Internacional sobre os Dados Genéticos Humanos, artigo 2.º (i)].

[184] Dados proteómicos humanos: informações relativas às proteínas de um indivíduo, incluindo a sua expressão, modificação e interação; [Declaração Internacional sobre os Dados Genéticos Humanos, artigo 2.º (ii)].

[185] Amostra biológica: qualquer amostra de material biológico (por exemplo células do sangue, da pele e dos ossos ou plasma sanguíneo) em que estejam presentes ácidos nucleicos e que contenha a constituição genética característica de um indivíduo; [Declaração Internacional sobre os Dados Genéticos Humanos, artigo 2.º (iv)].

Relativamente à informação genética, o Conselho Nacional de Ética para as Ciências da Vida (CNECV) emitiu um parecer[186] aquando da ratificação do Protocolo Adicional à CDHBM[187], no qual exprime "alguma preocupação relativamente ao uso impróprio dos testes genéticos, quando não são usados para fins relacionados com a saúde e quando não são enquadrados por consultas de aconselhamento genético, pelo que se pretende assegurar a proteção da informação obtida através da sua realização" (p. 7). Não obstante essa apreciação, o CNECV deu parecer favorável aos valores éticos acolhidos no Protocolo Adicional à CDHBM, que sublinha o respeito pelos princípios do primado do ser humano, da não discriminação, da não estigmatização e da reserva da vida privada (p. 8). Não obstante os receios manifestados, o referido Protocolo enfatiza os benefícios decorrentes da genética, nomeadamente dos testes genéticos, abrindo caminho para o que se designa por "medicina de precisão" ou "medicina personalizada".

Tal como aludido anteriormente, no plano europeu, o sector da saúde assume uma especial relevância em matéria de proteção de dados pessoais e no Art.º 9º n.º 1 do RGPD foi consagrado o princípio geral da proibição de tratamento de determinadas categorias especiais de dados, como os genéticos, biométricos, relativos à saúde ou relativos à vida sexual ou orientação sexual de uma pessoa.

A informação de saúde integra, nos termos do RGPD uma categoria especial de dados pessoais que são objeto de especial proteção. Porém, à luz das exceções previstas no n.º 2 do Art.º 9.º, tanto os dados de saúde, como os dados genéticos podem ser tratados quando se aplique um dos seguintes fundamentos de licitude:

a) Consentimento explícito do utente/portador de doença [alínea a) do n.º 2 do Art.º 9.º do RGPD];
b) Proteção de interesses vitais do utente ou de um terceiro, no caso de o titular dos dados estar fisicamente ou legalmente incapacitado de dar o seu consentimento [alínea c) do n.º 2 do Art.º 9.º do RGPD];
c) Medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamento de saúde e para gestão de sistemas e serviços de saúde [alínea h) do n.º 2 do Art.º 9.º do RGPD];
d) Interesse público no domínio da saúde pública [alínea i) do n.º 2 do Art.º 9.º do RGPD].

[186] Conselho Nacional de Ética para as Ciências da Vida (CNECV). Relatório e Parecer sobre a ratificação do Protocolo Adicional à Convenção para a Proteção dos Direitos do Homem e a Biomedicina (CDHBM) referente aos Testes Genéticos para fins relacionados com a Saúde, 84/CNECV/2015.

[187] Portugal assinou em 17 de março de 2015

Importa, no entanto, considerar que a cedência e/ou portabilidade da informação de saúde não pode, à luz do ordenamento jurídico vigente, ser considerado um ato meramente administrativo, que possa ser confiado ou executado por um funcionário do secretariado administrativo, pois o mesmo envolve, em primeiro lugar, decisões quanto ao preenchimento dos requisitos jurídicos de legitimidade, depois decisões médicas quanto à aplicação ou não do conceito de privilégio terapêutico e, finalmente, uma seriação daquelas que são as anotações pessoais dos médicos e as informações prestadas por terceiros e/ou relativas a terceiros.

O RGPD introduziu alterações significativas com implicações estruturais no funcionamento das organizações, que não cabe no âmbito do presente estudo, exigindo aos prestadores de cuidados de saúde, independentemente da sua natureza jurídica ou dimensão, uma adequação exigente e cuidada dos seus processos de tratamento de dados pessoais, sempre visando a garantia dos direitos e liberdades dos titulares desses dados.

5. Princípios éticos aplicáveis à prática clínica e à investigação médica

A *Declaração de Helsínquia, Princípios Éticos para a Investigação Médica em Seres Humanos* (versão de outubro 2013), defende que devem ser tomadas todas as precauções para proteger a privacidade de cada sujeito de investigação e a confidencialidade dos seus dados pessoais. No mesmo sentido, a *Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às aplicações da Biologia e da Medicina: Convenção sobre os Direitos do Homem e a Biomedicina (CDHBM)*[188], dispõe no Art.º 1.º que «As Partes na presente Convenção protegem o ser humano na sua dignidade e na sua identidade e garantem a toda a pessoa, sem discriminação, o respeito pela sua integridade e pelos seus outros direitos e liberdades fundamentais face às aplicações da biologia e da medicina.» e no Art.º 3.º prevê o acesso equitativo no acesso à saúde de qualidade apropriada.

[188] Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às aplicações da biologia e da medicina: convenção sobre os direitos do homem e a biomedicina.

Dos estudos realizados, verifica-se que os dilemas éticos na prática clínica provocados pelos avanços da ciência constituem a regra, quando outrora eram a exceção. No presente, são "enfrentados por todos os profissionais que se dedicam à prática da arte médica."[189]. Esses dilemas têm exigido uma maior atuação de "comités de ética" ou "conselhos de éticas" nas instituições, bem como a criação de códigos de ética, que orientam o cumprimento dos padrões éticos e legais, pelos profissionais de saúde, bem como o cumprimento da legislação aplicável à investigação científica.

A *Declaração de Helsínquia da Associação Médica Mundial sobre os Princípios Éticos Aplicáveis às Investigações Médicas sobre Sujeitos Humanos*, adotada em 1964[190], na versão atual, ocupa-se desta temática e reforça que «A investigação médica está sujeita a padrões éticos que promovem e garantem o respeito por todos os seres humanos e protegem a sua saúde e direitos.» (nº 7). A Declaração enuncia que, «Embora o objetivo primário da investigação médica seja gerar novo conhecimento, essa finalidade nunca prevalece sobre os direitos e interesses individuais dos participantes na investigação» (n.º 8). Sustenta ainda que, é um «dever dos médicos que participam em investigação médica proteger a vida, a saúde, a dignidade, a integridade, o direito à autodeterminação, a privacidade e a confidencialidade da informação pessoal dos participantes.» (n.º 9). É ao médico e ao profissional de saúde que cabe a responsabilidade de proteger os participantes sujeitos de investigação, não sendo aceitável a transferência para o sujeito de investigação, mesmo que este tenha dado consentimento.

O progresso da ciência assenta na investigação clínica, sendo defensável que os benefícios daí resultantes, devam ser partilhados com a sociedade no seu todo e, em particular com os países em desenvolvimento. Partindo dessa premissa, a *Declaração Universal sobre Bioética e Direitos Humanos*, adotada pela Conferência Geral da UNESCO em 11 de novembro de 1997, apresenta as várias formas de concretizar esses benefícios, designadamente através do acesso a cuidados de saúde de qualidade; fornecimento de novos produtos e meios terapêuticos ou diagnósticos, resultantes da investigação e apoio aos serviços de saúde.

[189] MARQUES FILHO, J. Bioética Clínica – Cuidando de Pessoas, Clinical Bioethics, p. 32.

[190] ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Helsínquia sobre os princípios éticos aplicáveis às investigações médicas sobre sujeitos humanos, adotada em 1964.

A saúde é essencial à própria vida e deve ser considerada um bem social e humano. A *Declaração Universal sobre o Genoma Humano e os Direitos Humanos*[191], alude aos benefícios dos progressos nas áreas da biologia, da genética e da medicina, relativos ao genoma humano, defendendo que esses benefícios «serão postos à disposição de todos, tendo devidamente em conta a dignidade e os direitos humanos de cada pessoa.» (al a) Art.º 12.º).

O Santo Padre Francisco recorda-nos

> "que a pesquisa científica e as inovações tecnológicas não estão desencarnadas da realidade nem são «neutrais»[192], mas estão sujeitas às influências culturais. Sendo atividades plenamente humanas, os rumos que tomam refletem opções condicionadas pelos valores pessoais, sociais e culturais de cada época. E o mesmo se diga dos resultados que alcançam: enquanto fruto de abordagens especificamente humanas do mundo envolvente, têm sempre uma dimensão ética, intimamente ligada às decisões de quem projeta a experimentação e orienta a produção para objetivos particulares."[193]

A *Declaração de Helsínquia da Associação Médica Mundial sobre os Princípios Éticos Aplicáveis às Investigações Médicas sobre Sujeitos Humanos*, adotada em 1964, anteriormente referida, defende que o «O objetivo primário da investigação médica em seres humanos é compreender as causas, a evolução e os efeitos das doenças e melhorar as intervenções preventivas, diagnósticas e terapêuticas (métodos, procedimentos e tratamentos). Mesmo as melhores e mais comprovadas intervenções atuais têm de ser continuadamente avaliadas através de investigação sobre a sua segurança, eficácia, eficiência, acessibilidade e qualidade» (n.º 6). No mesmo sentido, a *Declaração Universal sobre o Genoma Humano e os Direitos Humanos*[194], defende que **«**Nenhuma investigação na área do genoma humano ou respetivas aplicações, em particular nas áreas da biologia, da genética e da medicina, deve prevalecer sobre o respeito pelos direitos humanos,

[191] Declaração Universal sobre o Genoma Humano e os Direitos Humanos.

[192] FRANCISCO, Carta enc. *Laudato si'* (24/V/2015), 114, in Mensagem do Dia Mundial da Paz, 01 de janeiro de 2024.

[193] FRANCISCO. Mensagem do Santo Padre para a celebração do Dia Mundial da Paz, 1 de janeiro de 2024.

[194] Declaração Universal sobre o Genoma Humano e os Direitos Humanos.

pelas liberdades fundamentais e pela dignidade das pessoas ou, se for caso disso, dos grupos de pessoas.» (Art.º 10.º) [195].

A Associação Médica Mundial (AMM) elaborou a Declaração de Helsínquia como um enunciado de princípios éticos para a investigação clínica envolvendo seres humanos, incluindo investigação sobre dados e material humano identificáveis. De entre esses princípios, destaca-se o *princípio da integridade da investigação,* motivado pela consciência da existência de casos de violação da transparência, qualidade e integridade da investigação científica. Pelos mesmos motivos, na última revisão da Declaração de Helsínquia, Princípios Éticos para a Investigação Médica em Seres Humanos (2013), os aspetos da investigação científica feita em seres humanos, mormente nos n.os 35 e 36, foram enfatizados[196].

O Regulamento europeu sobre ensaios clínicos de medicamentos de uso humano (Regulamento (UE) N.º 536/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014), exige a garantia, robustez e fiabilidade do ensaio. Com efeito, a ética da investigação visa os seguintes objetivos: (i) defender a correção dos dados recolhidos; (ii) assegurar o prestígio e a qualidade da investigação clínica; (iii) garantir a qualidade dos produtos ou processos (*maxime* medicamentos) que resultam do estudo clínico e ainda a segurança e a saúde dos próprios participantes no ensaio clínico.

O princípio da integridade da investigação possui duas dimensões: (i) ao nível "supra-individual", fazendo o contraponto com o princípio do respeito pela intimidade da vida privada e familiar; (ii) ao nível pessoal-individual que participa no estudo clínico, obrigando a uma ponderação ética entre dois interesses ou valores da própria pessoa que consentiu participar num estudo clínico. Daqui resulta a possibilidade de interesses conflituantes (individual/comunitários), sendo admitido pela ética em investigação, o imperativo segundo o qual o bem-estar da sociedade e da ciência não prevalecem sobre o bem-estar do indivíduo, em conformidade com o Art.º 2.º da Convenção sobre os Direitos do Homem e a Biomedicina, que aí consagra o «primado do ser humano». No mesmo sentido, «Embora o objetivo primário da investigação médica seja gerar novo conhecimento, essa finalidade

[195] Idem Ibidem.

[196] ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Helsínquia sobre os princípios éticos aplicáveis às investigações médicas sobre sujeitos humanos, adotada em 1964.

nunca prevalece sobre os direitos e interesses individuais dos participantes na investigação.» (n.º 8 da Declaração de Helsínquia).

6. Bioética e o princípio da autonomia: o consentimento informado

O contributo da bioética para a autodeterminação da pessoa foi por nós abordado numa fase inicial do presente estudo. Aí ficou vertido, que a aplicação das novas tecnologias nos vários domínios da nossa vida, deve assentar no princípio da dignidade da pessoa humana, princípio estruturante que é reciprocamente influenciado pela autonomia pessoal, um princípio bioético que se traduz na defesa da autodeterminação de cada pessoa, em tomar decisões em relação à sua vida e em concreto à saúde.

Porém, o exercício da razão moral e da autodeterminação é condicionada por fatores diversos, de índole biológica, económica e social, sendo necessário atender a todos os elementos de ordem social e às demais fragilidades do ser humano. Ou seja, à luz do princípio da autonomia do ser humano extraímos uma regra geral sobre o consentimento. A esse propósito, o Regulamento n.º 707/2016, de 21 de julho, Regulamento de Deontologia Médica, refere no Art. 20.º que, «O consentimento do doente só é válido se este, no momento em que o dá, tiver capacidade de decidir livremente, se estiver na posse da informação relevante e se for dado na ausência de coações físicas ou morais.». Ou seja, o princípio da autonomia releva, mesmo nas situações de maior vulnerabilidade e dependência.

A Convenção para a Protecção dos Direitos do Homem e da Dignidade do ser Humano face às aplicações da Biologia e da Medicina: Convenção sobre os Direitos do Homem e a Biomedicina prevê no Art.º 5.º que, **«**Qualquer intervenção no domínio da saúde só pode ser efectuada após ter sido prestado pela pessoa em causa o seu consentimento livre e esclarecido. Esta pessoa deve receber previamente a informação adequada quanto ao objectivo e à natureza da intervenção, bem como às suas consequências e riscos. A pessoa em questão pode, em qualquer momento, revogar livremente o seu consentimento». No mesmo sentido, o Art.º 6.º da *Declaração Universal sobre Bioética e Direitos Humanos*, sublinha que,

> «1. Qualquer intervenção médica de carácter preventivo, diagnóstico ou terapêutico só deve ser realizada com o

> consentimento prévio, livre e esclarecido da pessoa em causa, com base em informação adequada. Quando apropriado, o consentimento deve ser expresso e a pessoa em causa pode retirá-lo a qualquer momento e por qualquer razão, sem que daí resulte para ela qualquer desvantagem ou prejuízo.
> 2. Só devem ser realizadas pesquisas científicas com o consentimento prévio, livre e esclarecido da pessoa em causa. A informação deve ser suficiente, fornecida em moldes compreensíveis e incluir as modalidades de retirada do consentimento. A pessoa em causa pode retirar o seu consentimento a qualquer momento e por qualquer razão, sem que daí resulte para ela qualquer desvantagem ou prejuízo. Excepções a este princípio só devem ser feitas de acordo com as normas éticas e jurídicas adoptadas pelos Estados e devem ser compatíveis com os princípios e disposições enunciados na presente Declaração, nomeadamente no Art.º 27º, e com o direito internacional relativo aos direitos humanos.»

A *Declaração Internacional sobre os Dados Genéticos Humanos*, no seu Art.º 8.º refere que «(a) O consentimento prévio, livre, informado e expresso, sem tentativa de persuasão por ganho pecuniário ou outra vantagem pessoal, deverá ser obtido para fins de recolha de dados genéticos humanos, de dados proteómicos humanos ou de amostras biológicas, quer ela seja efectuada por métodos invasivos ou não-invasivos, bem como para fins do seu ulterior tratamento, utilização e conservação, independentemente de estes serem realizados por instituições públicas ou privadas. Só deverão ser estipuladas restrições ao princípio do consentimento por razões imperativas impostas pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos.».

No mesmo sentido, o RGPD prevê no Art.º 7.º as condições aplicáveis ao consentimento, sendo exigido ao responsável pelo tratamento não somente a prova da recolha do consentimento, mas igualmente a prova "que o consentimento foi efetivamente assentido."[197]

7. Vulnerabilidade como um conceito ético-jurídico

As questões éticas suscitadas pela medicina, ciências da vida e tecnologias associadas na sua aplicação aos seres humanos abordadas anteriormente, estão previstas na *Declaração Universal sobre Bioética e Direitos Humanos,* adotada em

[197] MENEZES CORDEIRO. 2021.p.121.

2005[198], instrumento que foi concebido em defesa do pleno respeito pela dignidade humana, direitos humanos e liberdades fundamentais.

Ao consagrar a bioética entre os direitos humanos internacionais e ao garantir o respeito pela vida dos seres humanos, a Declaração defende que «Os interesses e o bem-estar do indivíduo devem prevalecer sobre o interesse exclusivo da ciência ou da sociedade.» (n.º 2 do Art.º 3.º). Reconhece a interligação que existe entre ética e direitos humanos no domínio específico da bioética e defende a maximização dos efeitos benéficos diretos e indiretos dos avanços dos conhecimentos científicos, da prática médica e das tecnologias que lhes estão associadas, aplicando-os aos doentes, participantes em investigações e outros indivíduos envolvidos, devendo minimizar qualquer efeito nocivo suscetível de afetar esses indivíduos (Art.º 4.º).

A Declaração consagra o respeito pela vulnerabilidade humana e integridade pessoal no Art.º 8.º, prevendo aí que «Na aplicação e no avanço dos conhecimentos científicos, da prática médica e das tecnologias que lhes estão associadas, deve ser tomada em consideração a vulnerabilidade humana. Os indivíduos e grupos particularmente vulneráveis devem ser protegidos, e deve ser respeitada a integridade pessoal dos indivíduos em causa.»

No plano nacional, a Constituição da República Portuguesa (CRP) acolhe no Art.º 1.º a dignidade da pessoa humana, princípio que acompanha o percurso vital de cada pessoa, nas suas múltiplas circunstâncias. Mariana Canotilho defende que "A *pessoa* constitucional é uma pessoa que *muda*, evolui e se transforma, passando por períodos de maior fragilidade, ou *vulnerabilidade*, mais ou menos duradouros, em que, à semelhança dos períodos da infância, juventude e terceira idade, necessita de uma *especial proteção constitucional*, de *direitos fundamentais específicos* e de políticas públicas próprias. São óbvios exemplos destas situações a deficiência (Art.º 71.º da CRP), a gravidez, a maternidade e a paternidade (Art.os 36.º e 68.º) e a doença (Art.º 64.º da CRP)"[199]. A autora refere as inúmeras disposições normativas positivadas no texto constitucional que se destinam a conferir direitos pessoais, laborais e de cidadania a qualquer pessoa. Na visão da autora, que acompanhamos de perto,

[198] Declaração Universal sobre Bioética e Direitos Humanos.

[199] CANOTILHO, Mariana. 2022, p. 146.

> "(…) A pessoa constitucional é, assim, multidimensional. Tem um nome, uma identidade, uma imagem (veja-se o Art.º 26.º da CRP); vive em família (Art.º 36.º), organiza-se em associações de diversa natureza (Art.º 46.º); instrui-se, aprende (Art.os 43.º, e 73.º a 76.º da CRP); trabalha (e, neste ponto, acentue-se a relevância fulcral do trabalho, no texto e no projeto político da Constituição, que se reflete no número e densidade de disposições constitucionais sobre a matéria, desde logo, todo o Capítulo III do Título II – direitos, liberdades e garantias dos trabalhadores, e os Art.os 58.º e 59.º da CRP)"[200].

A vulnerabilidade humana é uma condição universal reconhecida também pela *Declaração Universal sobre o Genoma Humano e os Direitos Humanos* (adotada pela Conferência Geral da UNESCO em 11 de novembro de 1997), que defende igualmente o direito à saúde como um dos direitos fundamentais de qualquer ser humano,

> "Reconhecendo que a investigação sobre o genoma humano e suas consequentes aplicações abre amplas perspetivas de progresso ao nível da melhoria da saúde dos indivíduos e da Humanidade no seu conjunto, mas sublinhando que tal investigação deve respeitar plenamente a dignidade humana, a liberdade e os direitos humanos, bem como a proibição de todas as formas de discriminação com base nas características genéticas," .

Os fundamentos expostos permitem-nos observar que a pessoa humana é um sujeito livre e racional, mas também vulnerável e dependente, designadamente em caso de doença, cuja vulnerabilidade convoca a intervenção do Estado na prestação de cuidados de saúde, destacando-se em Portugal, o Serviço Nacional de Saúde e, mais recentemente, com a mobilização por parte dos municípios.

8. Governação Europeia de Dados

Existe uma apreensão relativa à eventual vulnerabilidade dos titulares dos dados pessoais e em especial dos dados relativos à saúde, face à criação dos prestadores

[200] Idem Ibidem.

de serviços de intermediação de dados, em execução do Regulamento (UE) 2022/868, de 30 de maio de 2022 (Governação Europeia de Dados)[201].

Se por um lado, com este novo instrumento, que entrou em vigor no dia 24 de setembro de 2023, se procura reforçar a capacidade de ação dos titulares dos dados, nomeadamente o controlo que os titulares exercem sobre os dados que lhes dizem respeito, por outro lado, faltam definir os requisitos relativos à fiabilidade da prestação dos serviços de intermediação de dados, necessários à segurança do tratamento dos dados, de modo a assegurar que os titulares dos dados e detentores dos dados, bem como os utilizadores de dados, exerçam o controlo sobre o acesso e a utilização dos seus dados, em conformidade com o direito da União.

Em termos gerais, os serviços de intermediação de dados e, em concreto dos dados pessoais relativos à saúde, irão desempenhar um papel fundamental na sociedade, com potencial para a mutualização eficiente desses dados, bem como uma maior facilidade de partilha bilateral de dados. O considerando 27 do Regulamento de Governação Europeia de Dados dispõe que, "(…) Os serviços de intermediação de dados poderão incluir as partilhas bilaterais ou multilaterais de dados ou a criação de plataformas ou de bases de dados que permitam a partilha ou a utilização conjunta de dados, bem como a criação de uma infraestrutura específica para a interligação dos titulares dos dados e dos detentores dos dados com os utilizadores de dados.". Trata-se de ativos que irão permitir a reutilização dos dados detidos por um organismo do setor público, realizada para fins comerciais, que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos e carece de mais informação relativamente à execução de interfaces técnicas e às condições técnicas e organizativas a aplicar.

A autoridade de controlo (a criar) poderá exigir a garantia de que não existem incentivos desajustados que levem os titulares dos dados a utilizarem esses serviços para disponibilizarem informações contra os seus próprios interesses. Tal poderá passar por informação a disponibilizar aos cidadãos, incluindo o aconselhamento sobre as utilizações possíveis dos seus dados, a fim de evitar práticas fraudulentas.

Um elemento fundamental para instaurar a confiança e aumentar o controlo, por parte dos detentores dos dados, dos titulares dos dados e dos utilizadores dos

[201] JOUE. Regulamento (UE) 2022/868 de 30 de maio de 2022.

dados, relativamente aos serviços prestados, passa pela garantia de neutralidade dos prestadores de serviços de intermediação de dados no que diz respeito aos dados trocados entre os detentores dos dados ou os titulares dos dados e os utilizadores dos dados. Por conseguinte, os prestadores de serviços de intermediação de dados, devem atuar como intermediários nas transações e não utilizar os dados trocados para qualquer outro fim.

O serviço de intermediação de dados pessoais relativos à saúde insere-se numa categoria específica de serviços de intermediação de dados. Estes prestadores de serviços procuram reforçar a capacidade de ação dos titulares dos dados, nomeadamente o controlo que as pessoas exercem sobre os dados que lhes dizem respeito. Nessa medida, para que se constitua como prestador de serviços de intermediação de dados relativos à saúde[202], sob jurisdição do Estado português, ser-lhe-á exigido: (i) a exequibilidade dos direitos dos titulares constantes do Capítulo III do Regulamento (UE) 2016/679, de 27 de abril (RGPD), nomeadamente o direito de dar e retirar o seu consentimento para o tratamento dos dados, o direito de acesso aos dados de que são titulares, o direito à retificação de dados pessoais inexatos, o direito ao apagamento dos dados ou o direito «a ser esquecido», o direito à limitação do tratamento e o direito à portabilidade dos dados, que permite aos titulares transferir os seus dados pessoais de um responsável pelo tratamento de dados para outro; (ii) a observância do procedimento de notificação à autoridade competente; (iii) a submissão ao controlo e supervisão do cumprimento dos requisitos previstos no Capítulo III do Regulamento de Governação Europeia de Dados.

A fim de aplicar o quadro de governação europeia de dados, foi criado o Comité Europeu da Inovação de Dados (*European Data Innovation Board*), sob a forma de um grupo de peritos, o qual irá facilitar a partilha de boas práticas em matéria de intermediação de dados, bem como, definir as prioridades em matéria de normas de interoperabilidade intersectoriais. De acordo com o considerando 53

[202] Qualquer prestador de serviços de intermediação de dados, deve seguir os modelos constantes do anexo do Regulamento de execução (UE) 2023/1622 da Comissão de 9 de agosto de 2023, relativo à conceção de logótipos comuns para identificar os prestadores de serviços de intermediação de dados e as organizações de altruísmo de dados reconhecidos na União, que entrou em vigor em 2023, e está acessível em: «https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023R1622». Importa nesta matéria referir que Portugal já tornou público o seu logótipo, acessível em: «https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union». A Comissão Europeia manterá um registo central dos intermediários de dados reconhecidos.

do Regulamento de Governação Europeia de Dados, o Comité Europeu da Inovação de Dados[203] deverá ser composto por representantes das autoridades competentes para serviços de intermediação de dados, bem como por vários subgrupos, incluindo um subgrupo para a participação das partes interessadas, composto por representantes pertinentes da indústria, como a saúde, o ambiente, a agricultura, os transportes, a energia, a indústria transformadora, os meios de comunicação social, os setores cultural e criativo e as estatísticas, bem como por representantes da investigação, do meio académico, da sociedade civil, dos organismos de normalização, dos espaços comuns europeus de dados pertinentes e de outras partes interessadas e terceiros pertinentes, nomeadamente organismos com competências específicas, como os serviços nacionais de estatística.

Considerações finais

Sob a Presidência espanhola do Conselho da União, no início de dezembro de 2023, o Conselho e o Parlamento chegaram a um acordo, ainda que provisório, sobre regras harmonizadas em matéria de IA. O projeto de regulamento visa garantir que os sistemas de IA colocados no mercado europeu e utilizados na União Europeia, ofereçam segurança e respeitem os direitos fundamentais, bem como os valores da União, estimule o investimento e a inovação na Europa. Fora do Regulamento Inteligência Artificial ficou a legislação relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade Civil da IA). Também nesta matéria foi alcançado, no dia 14 de dezembro de 2023, um acordo político entre os Estados-Membros.

O novo contexto, traz obrigatoriamente ao debate os desafios éticos da transformação digital, a proibição do tratamento de categorias especiais de dados pessoais, bem como uma reflexão sobre a vulnerabilidade como um conceito ético-jurídico. Dos estudos realizados, verifica-se que os dilemas éticos na prática clínica provocados pelos avanços da ciência constituem a regra, quando outrora eram a exceção. Esses dilemas têm exigido uma maior atuação de "comités de

[203] O Comité Europeu da Inovação de Dados reuniu pela primeira vez no dia 13 de dezembro de 2023, informação que poderá ser acedida em: «https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3903».

ética" ou "conselhos de éticas" nas instituições, bem como a criação de códigos de ética, que orientam o cumprimento dos padrões éticos e legais, pelos profissionais de saúde, bem como o cumprimento da legislação aplicável à investigação científica.

Cumpre-nos sublinhar que a pessoa humana é um sujeito livre e racional, mas também vulnerável e dependente, designadamente em caso de doença, cuja vulnerabilidade convoca em Portugal, a intervenção do Estado na prestação de cuidados de saúde, destacando-se em particular o Serviço Nacional de Saúde, tendo a Estratégia Nacional de Territórios Inteligentes, mobilizado a atuação dos municípios em torno da oferta de cuidados de saúde.

Por fim, reforçamos a apreensão anteriormente demonstrada, relativamente à vulnerabilidade dos titulares dos dados pessoais face ao tratamento dos seus dados de saúde, por parte de prestadores de serviços de intermediação de dados privado, em execução do Regulamento Governação Europeia de Dados. Se por um lado esse Regulamento procura reforçar o controlo que os titulares deveriam exercer sobre os dados que lhes dizem respeito, por outro lado não foram ainda definidos os requisitos relativos à fiabilidade da prestação dos serviços de intermediação de dados.

Referências Bibliográficas

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA (AMA). Estratégia Nacional de Territórios Inteligentes- ENTI (2023-2030), Área Governativa da Digitalização e da Modernização Administrativa. Dezembro 2023. Disponível em:

HTTPS://WWW.AMA.GOV.PT/DOCUMENTS/24077/320185/ENTI_RCM_V2_ATUALIZADO.PDF/634A2167-0E64-48E5-9DDC-EF1FD3FC0CA8

ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Helsínquia sobre os princípios éticos aplicáveis às investigações médicas sobre sujeitos humanos, adotada em 1964. Disponível em: https://www.ucp.pt/sites/default/files/2019-03/declaracao-de-helsinquia_2013.pdf

CANOTILHO, Mariana. «A vulnerabilidade como conceito constitucional: Um elemento para a construção de um constitucionalismo do comum», OÑATI SOCIO-LEGAL SERIES VOLUME 12, ISSUE 1 (2022), 138–163 publicado em fevereiro de 2022, p. 146. Disponível em: file:///C:/Users/cristina.caldeira/Downloads/pdf-12-1-canotilho-osls%20(3).pdf

CONSELHO NACIONAL DE ÉTICA PARA AS CIÊNCIAS DA VIDA (CNECV). Relatório e Parecer sobre a ratificação do Protocolo Adicional à Convenção para a Proteção dos Direitos do Homem e a Biomedicina (CDHBM) referente aos Testes Genéticos para fins relacionados com a Saúde, 84/CNECV/2015. Disponível em: https://www.cnecv.pt/pt/deliberacoes/pareceres/parecer-n-o-84-cnecv-2015-sobre-a-ratificacao-do-protocolo-adici?download_document=3202&token=e848d37cdb49de5145fcffa922383687

CONVENÇÃO PARA A PROTEÇÃO DOS DIREITOS DO HOMEM E DA DIGNIDADE DO SER HUMANO face às aplicações da biologia e da medicina: convenção sobre os direitos do homem e a biomedicina. Disponível em:

https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_dh_biomedicina.pdf

DECLARAÇÃO INTERNACIONAL SOBRE OS DADOS GENÉTICOS HUMANOS, adotada pela Conferência Geral da UNESCO em 16 de outubro de 2003. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_inter_dados_genericos.pdf

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS (DUDH). Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/declaracao_universal_dos_direitos_do_homem.pdf

DECLARAÇÃO UNIVERSAL SOBRE BIOÉTICA E DIREITOS HUMANOS

Disponível em: https://www.ufp.pt/app/uploads/2019/06/declara%C3%A7%C3%A3o-universal-sobre-bio%C3%A9tica-e-direitos-humanos.pdf

DECLARAÇÃO UNIVERSAL SOBRE O GENOMA HUMANO E OS DIREITOS HUMANOS. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/decl-genomadh.pdf

FRANCISCO. Discurso aos participantes no Encontro dos «Minerva Dialogues» (27/III/2023), referido na mensagem do Santo Padre Francisco para a celebração do dia mundial da paz, 1 de janeiro de 2024. Disponível em: https://www.vatican.va/content/francesco/pt/messages/peace/documents/20231208-messaggio-57giornatamondiale-pace2024.html

GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE INTELIGÊNCIA ARTIFICIAL, *Orientações éticas para uma inteligência artificial*, p. 14. Disponível em: file:///E:/EthicsguidelinesfortrustworthyAI-PTpdf%20(1).pdf.

HOFFMANN-REIM, WOLFGANG. *Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito*, Editora Forense, Rio de Janeiro, 2021, pp. 11-13.

JORNAL OFICIAL DA UNIÃO EUROPEIA (JOUE)

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados): Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

Regulamento (ue) 2022/868 do parlamento europeu e do conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento Governação de Dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R0868

Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da união. Bruxelas, 21.4.2021. COM(2021) 206 final. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF

Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade da IA). Bruxelas, 28.9.2022 COM(2022) 496 final. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496

MARQUES FILHO, J. Bioética Clínica – Cuidando de Pessoas, Clinical Bioethics – Caring for People in Rev Bras Reumatol, v. 48, n.1, p. 31-33, jan/fev, 2008, p. 32. Disponível em: https://www.scielo.br/j/rbr/a/yfXrdNrjhZpDZsCdNFwgXRw/?format=pdf

MENEZES CORDEIRO. *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*. Almedina, Coimbra, 2021.p.121.

NAÇÕES UNIDAS. *Interim Report: Governing AI for Humanity*, *AI* Advisory Body, dezembro 2023. Disponível em: https://www.un.org/ai-advisdory-body

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial (2020/2015(INI)). Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PT.html

VITORINO., G; CORDEIRO, J.; MAGALHÃES, T.. «A transformação digital nas suas diversas dimensões», in *Transformação digital em Saúde*. Associação Portuguesa de Administradores Hospitalares, editora Almedina, Coimbra (2021).

O *day after* do Acórdão do Tribunal Constitucional n.º 268/2022

Duarte Rodrigues Nunes*

Introdução

No transato ano de 2022, pouco tempo após a prolação do Acórdão do TC n.º 268/2022, escrevemos um artigo em que formulámos fortes críticas a este aresto[204]. Na sequência desse artigo, fomos convidados para proferir algumas palestras sobre o tema, uma das quais no Centro de Estudos Judiciários, no âmbito da formação contínua de Magistrados. Subsequentemente, fomos ouvidos pelo Grupo de Trabalho dos Metadados da 1.ª Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República, no âmbito do procedimento legislativo tendente à reformulação da Lei n.º 32/2008, de 17 de julho, após a prolação do Acórdão do TC n.º 268/2022, tendo então elaborado um pequeno estudo, que é o ponto de partida para o presente artigo.

* Professor Associado da Universidade Europeia. Professor Associado Convidado da Universidade Lusíada – Angola e no Instituto Superior de Psicologia Aplicada (ISPA). Doutor em Direito pela Faculdade de Direito de Lisboa. Investigador do IDPCC e do CIJIC. Jurisconsulto. Conferencista. Exerceu as funções de Juiz de Direito entre setembro de 2005 e janeiro de 2022, estando atualmente em situação de licença sem retribuição.

Este artigo foi entregue para publicação no dia 13 de novembro de 2023.

204 DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 9-58.

1. O Acórdão Digital Rights do Tribunal de Justiça da União Europeia e o Acórdão do Tribunal Constitucional n.º 268/2022

No rescaldo dos terroristas de Madrid (11 de março de 2004) e de Londres (7 de julho de 2005), em que foi a reconstituição das comunicações eletrónicas entre os vários intervenientes das redes terroristas em causa que permitiu às autoridades perceberem as relações existentes entre eles, o Parlamento Europeu e o Conselho adotaram a Diretiva 2006/24/CE, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A Diretiva 2006/24/CE, que visou harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de dados de tráfego, dados de localização relativos pessoas singulares e/ou a pessoas coletivas e dados conexos necessários para identificar o assinante ou o utilizador registado por eles gerados ou tratados (correntemente designados como metadados[205]) para fins de investigação, deteção e repressão de crimes graves, tal como definidos no Direito nacional de cada Estado-Membro, obrigou os Estados-Membros a tomarem medidas para garantir a conservação dos dados necessários para:

a) encontrar e identificar a fonte e/ou o destino de uma comunicação;
b) identificar a data, a hora e a duração de uma comunicação;
c) identificar o tipo de comunicação;
d) identificar o equipamento de telecomunicações dos utilizadores ou o que se considera ser o seu equipamento; e
e) identificar a localização do equipamento de comunicação móvel (incluindo no caso de chamadas telefónicas falhadas), quando gerados ou tratados e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da Internet) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações que estejam sob a jurisdição do

[205] Sem prejuízo do escasso rigor dessa designação.

Estado-Membro em questão, no contexto da oferta de serviços de comunicação.

Tal Diretiva excluía expressamente do seu âmbito de aplicação a conservação de dados de conteúdo de comunicações (cfr. arts. 1.º, n.º 2, e 5.º, n.º 2).

A Diretiva 2006/24/CE foi transposta para o Direito português através da Lei n.º 32/2008.

Todavia, a Diretiva 2006/24/CE foi declarada inválida pelo TJUE, no âmbito de um reenvio prejudicial ao abrigo do art. 267.º do TFUE, através do seu Acórdão 8 de abril de 2014, Digital Rights Ireland Ltd e Kärntner Landesregierung[206].

Nesse aresto, o TJUE entendeu que a conservação dos dados referidos na Diretiva e o acesso das autoridades a esses dados restringem, de forma intensa (embora sem afetar o seu conteúdo essencial), os direitos tutelados pelos arts. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), sendo que, nos termos do artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades garantidos pela CDFUE deve estar prevista na lei e respeitar o conteúdo essencial desses direitos e liberdades e, por força dos ditames do princípio da proporcionalidade, só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

E, nessa conformidade, o TJUE considerou que, apesar de não ocorrer qualquer restrição do conteúdo essencial dos referidos direitos fundamentais e de estar em causa a prossecução de fins legítimos (a resposta à criminalidade grave e, em última análise, a salvaguarda da segurança pública), a Diretiva 2006/24/CE restringia, de forma desproporcionada, os mencionados direitos fundamentais, uma vez que:

a) abrangia, de uma forma indiscriminada, todas as pessoas que utilizassem serviços de comunicações eletrónicas, inclusivamente pessoas em relação às quais não existiam indícios de que o seu comportamento pudesse ter um nexo, ainda que indireto ou longínquo, com infrações graves e sem prever qualquer exceção quanto a comunicações

[206] Usualmente designado Acórdão Digital Rights.

abrangidas pela proteção do segredo profissional;

b) não exigia nenhuma relação entre os dados conservados e uma ameaça para a segurança pública nem limitava a conservação a dados relativos a um período de tempo, a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de alguma forma, numa infração grave nem a dados relativos a pessoas cuja conservação pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves;

c) não estabelecia critérios objetivos que permitissem delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior à prevenção, deteção ou punição de infrações graves;

d) não limitava o acesso e a utilização posterior dos dados conservados à prevenção e à deteção de crimes graves nem estabelecia critérios objetivos que permitam limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário tendo em conta o objetivo prosseguido;

e) não exigia que o acesso aos dados conservados dependesse de um pedido fundamentado no âmbito de procedimentos de prevenção ou de deteção de crimes ou de uma ação penal e fosse objeto de controlo prévio por um órgão jurisdicional ou entidade administrativa independente e também não obrigava os Estados-Membros a preverem esses requisitos no seu Direito interno;

f) no que respeita à duração da conservação dos dados, que impunha que fosse fixada entre 6 e 24 meses, não procedia a qualquer distinção entre as categorias de dados em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa nem impunha que a determinação do período de conservação deveria basear-se em critérios objetivos, a fim de garantir que se limitava ao estritamente necessário; e

g) quanto à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas, (1) não obrigava os Estados-Membros a estabelecerem regras específicas e adaptadas à grande quantidade de dados cuja conservação era imposta, ao caráter

sensível desses dados e ao risco de acesso ilícito aos mesmos, (2) não garantia a aplicação, pelos referidos fornecedores, de um nível particularmente elevado de proteção, (3) não impunha a destruição definitiva dos dados no termo do período de conservação dos mesmos e (4) não impunha a obrigação de os metadados serem conservados no território da União Europeia (pelo que não se poderia considerar que estivesse plenamente garantida a fiscalização do respeito das exigências de proteção e de segurança por uma entidade independente, tal exigido pelo art. 8.º, n.º 3, da CDFUE).

Na sequência deste acórdão do TJUE, passou a discutir-se se a Lei n.º 32/2008 era, ou não, incompatível com o Direito da União Europeia e se, consequentemente, a conservação de dados à luz dessa Lei era, ou não, admissível à luz da e da CDFUE[207].

Contudo, a principal consequência, entre nós, do Acórdão Digital Rights, foi o Acórdão do TC n.º 268/2022.

Assim, por via do aludido aresto, o TC, embora com um voto de vencido, declarou inconstitucionais, com força obrigatória geral:

a) a norma constante do art. 4.º da Lei n.º 32/2008, conjugada com o art. 6.º da mesma Lei, por violação do disposto nos arts. 35.º, n.ºs 1 e 4, e 26.º, n.º 1, em conjugação com o art. 18.º, n.º 2, todos da CRP; e
b) a norma constante do art. 9.º da Lei n.º 32/2008 (na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros), por violação do disposto nos arts. 35.º, n.º 1, e 20.º, n.º 1, em conjugação com o art. 18.º, n.º 2, todos da CRP[208].

---

[207] *Vide* a este respeito, com maiores desenvolvimentos, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 22-23.

[208] Note-se, porém, que o TC (tal como o TJUE, embora relativamente à CDFUE), em momento algum considerou inconstitucional a utilização probatória de metadados nem a obtenção de metadados em tempo real (no mesmo sentido, RUI CARDOSO, "A conservação e a

O Acórdão n.º 268/2022 foi prolatado no âmbito de um pedido de declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, em sede de fiscalização abstrata sucessiva à luz do art. 281.º da CRP, formulado pela Provedora da Justiça.

Esta declaração da inconstitucionalidade veio suscitar a questão da admissibilidade, ou não, da obtenção e valoração, nos processos em curso, de metadados que tenham sido conservados pelos respetivos operadores e das provas obtidas através desses metadados. E, ainda mais grave, veio abrir a possibilidade de, se forem interpostos recursos de revisão ao abrigo do art. 449.º, n.º 1, als. e) e f), do CPP que sejam julgados procedentes, serem revertidas condenações transitadas em julgado em processos nos quais, em observância de todas as garantias e esgotados todos os mecanismos de recurso de que os arguidos tenham decidido lançar mão, se provou, para além da dúvida razoável, o cometimento do crime ou dos crimes pelos quais foram condenados[209].

2. A jurisprudência do Tribunal de Justiça da União Europeia posterior ao Acórdão Digital Rights

Após ter anulado a Diretiva 2006/24/CE, o TJUE passou a apreciar a questão da conservação de metadados para efeitos de investigação criminal com base no art. 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, interpretado à luz dos arts. 7.º, 8.º e 52.º, n.º 1, da CDFUE.

Assim, no Acórdão Tele2 Sverige AB e Secretary of State for the Home Department, o TJUE entendeu que:

---

utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 35 e ss.).

[209] No entanto, tais recursos têm sido julgados improcedentes pelo STJ (cfr., entre outros, Acórdãos do STJ de 21/09/2022, 10/11/2022, 19/01/2023, 01/02/2023, 11/05/2023, 21/06/2023 e 29/06/2023), com fundamento no disposto no art. 282.º, n.º 3, 2.ª parte, da CRP, porquanto o TC, no Acórdão n.º 268/2022 não afastou a ressalva dos casos julgados, entendimento cuja bondade não cumpre analisar no âmbito do presente artigo, atento o respetivo objeto.

a) A CDFUE proíbe a conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica;
b) A CDFUE impõe que os dados sejam conservados no território da União Europeia; e
c) A CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente.

No Acórdão Ministerio Fiscal, o TJUE entendeu que a CDFUE permite o acesso das autoridades públicas a dados de base como o apelido, o nome próprio, a morada dos titulares dos cartões SIM ativados num telemóvel roubado, para efeitos de luta contra a criminalidade grave.

No Acórdão Privacy International, o TJUE considerou que a CDFUE proíbe a imposição, aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, da transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações.

No Acórdão La Quadrature du Net, o TJUE entendeu que a CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo, mas permite:

a) A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave e que seja real e atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva (por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos) e essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;
b) A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra

a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado; e

c) A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública.

No Acórdão Prokuratuur, o TJUE considerou que:

a) A CDFUE proíbe o acesso de autoridades públicas a dados de tráfego ou de localização para fins de prevenção, investigação, deteção e perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública, independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis sobre tal período; e
b) A atribuição da competência ao MP para autorizar o acesso aos dados de tráfego e aos dados de localização para fins de investigação criminal viola a CDFUE, pois a missão do MP é dirigir a investigação e exercer a ação penal.

No Acórdão G. D. e Commissioner of An Garda Síochána, o TJUE entendeu que a CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

a) A conservação seletiva de dados de tráfego e de dados de localização, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou

através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

b) A conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, por um período temporalmente limitado ao estritamente necessário; e

c) A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional,

desde que (1) esteja assegurado, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e (2) as pessoas visadas disponham de garantias efetivas contra eventuais abusos.

Finalmente[210], no Acórdão SpaceNet e Telekom Deutschland, o TJUE considerou que a CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

a) A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave e que seja real e atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva (por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos) e essa conservação apenas ocorra durante um período

[210] Posteriormente a este aresto, o TJUE proferiu o Acórdão A. G. e Lietuvos Respublikos generalinė prokuratūra, em que, apesar de versar sobre a utilização de metadados conservados, o Tribunal analisa uma questão diversa, mais concretamente, a de saber se é admissível, à luz da CDFUE, a utilização, em investigações relativas a ilícitos disciplinares relativos a atos de corrupção, de metadados que haviam sido conservados pelos prestadores de serviços de comunicações eletrónicas. O TJUE considerou que tal não é admissível, por violação dos arts 7.º, 8.º e 52.º, n.º 1, da CDFUE, uma vez que não estava em causa o afastamento de qualquer ameaça à segurança interna ou à segurança pública nem a luta contra a criminalidade grave.

temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;

b) A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

c) A conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, por um período temporalmente limitado ao estritamente necessário; e

d) A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública,

desde que (1) esteja assegurado, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e (2) as pessoas visadas disponham de garantias efetivas contra eventuais abusos.

Em suma, de acordo com a jurisprudência do TJUE, em matéria de conservação de metadados, a CDFUE impõe que os dados sejam conservados no território da União Europeia e proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

1. A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave, real e atual ou previsível, desde que essa conservação apenas ocorra durante um

período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça, contanto que a decisão que determina a conservação seja efetivamente fiscalizada por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos;

2. A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;
3. A conservação generalizada e indiferenciada, por um período temporalmente limitado ao estritamente necessário, dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional; e
4. A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública.

E, relativamente ao acesso aos metadados conservados, a CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (que não inclui o MP, pois é o titular da ação penal).

3. A jurisprudência dos Tribunais Judiciais portugueses na sequência do Acórdão do Tribunal Constitucional n.º 268/2022 em matéria de obtenção e/ou valoração de metadados conservados

No seguimento do Acórdão do TC n.º 268/2022, surgiram, na jurisprudência dos Tribunais comuns, dois entendimentos em matéria de obtenção e/ou valoração de metadados conservados.

Assim, para um primeiro entendimento[211], por força da declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, não é admissível obter e a valorar, em processos penais, metadados conservados à luz da Lei n.º 41/2004, de 18 de agosto, pelos prestadores de serviços de comunicações eletrónicas e obtidos à luz do art. 189.º, n.º 2, do CPP ou da Lei n.º 109/2009, de 15 de setembro, argumentando-se que:

a) Dado que a Lei n.º 41/2004 é relativa à proteção contratual no contexto das relações estabelecidas entre as empresas fornecedoras de serviços de comunicações eletrónicas e os seus clientes, não é lícito recorrer a este diploma para efeitos de investigação criminal[212];
b) Aplicar o regime dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009, significaria "*deixar entrar pela janela*" aquilo a que o Acórdão do TC n.º 268/2022 "*fechou a porta*", pois o regime que resultaria da aplicação dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009 padece da mesma falta de garantias, no plano da investigação criminal, que levou à declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei nº 32/2008[213];
c) Aplicar a Lei n.º 109/2009 implicaria defraudar o espírito do legislador, pois o desaparecimento da norma especial (*in casu*, os arts. 3.º e 9.º da Lei n.º

[211] Acolhido nos Acórdãos da RL de 25/10/2022, da RP de 07/09/2022, 07/12/2022 e 24/05/2023, da RC de 12/10/2022 e da RE de 25/10/2022, 28/02/2023, 09/05/2023 e 12/09/2023.

[212] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[213] Cfr. Acórdão da RP de 07/12/2022.

32/2008) não legitima a aplicação da norma geral (*in casu*, as normas da Lei n.º 109/2009)[214];

d) Os Tribunais não podem substituir-se ao legislador, suprindo omissões de onde resultam graves inconvenientes para a investigação criminal[215];

e) Dado que não existe qualquer identidade formal ou material entre o catálogo de crimes do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e o catálogo de crimes dos arts. 187.º, n.º 1, e 189.º do CPP, não há revogação do segundo pelo primeiro dos dois regimes e, por isso, não se tem de aplicar, por repristinação, nenhuma norma do CPP (o que, de resto, implicaria o desrespeito pela opção do legislador de ter criado um catálogo mais restrito no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 em vez de considerar como "crimes graves" os crimes constantes do catálogo do n.º 1 do art. 187.º do CPP)[216];

f) "Caindo" a Lei n.º 32/2008 e na impossibilidade de aplicação do CPP e da Lei n.º 41/2004, recorrer às normas da Lei n.º 109/2009 seria seguir um caminho espúrio, tendo em conta a declaração de inconstitucionalidade e os fundamentos que a determinaram, não sendo lícito recorrer a "atalhos" como a invocação do disposto no art. 189.º do CPP ou na Lei n.º 109/2009 (para mais quando o art. 11.º, n.º 2, desta Lei determina que o disposto nos arts. 12.º a 19.º dessa Lei não prejudica o regime da Lei n.º 32/2008)[217];

g) Tendo em conta os fundamentos da declaração de invalidade da Diretiva 2006/24/CE pelo TJUE, o regime da Lei n.º 32/2008 teria de ser ainda mais restritivo (e daí a declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º desta Lei), sendo certo que o regime do art. 189.º, n.º 2, do CPP é menos exigente do que o regime da Lei n.º 32/2008[218]; e

h) Obter ou valorar metadados conservados com base no art. 189.º, n.º 2, do CPP, na Lei n.º 41/2004 e na Lei n.º 109/2009 levaria a que a

[214] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[215] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[216] Cfr. Acórdão da RC de 12/10/2022.

[217] Cfr. Acórdão da RC de 12/10/2022.

[218] Cfr. Acórdão da RC de 12/10/2022.

declaração de inconstitucionalidade produzisse o efeito contrário àquele que pretendeu (pois permitiria a aplicação de um regime menos restritivo do que o regime dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008)[219].

Diversamente, para um segundo entendimento[220], apesar da declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, a obtenção e a valoração, em processos penais, de metadados conservados à luz da Lei n.º 41/2004, de 18 de agosto, pelos prestadores de serviços de comunicações eletrónicas, para fins de faturação dos serviços prestados continua a ser admissível[221], porquanto essas normas não foram declaradas inconstitucionais pelo TC.

4. A jurisprudência do Tribunal Europeu dos Direitos Humanos

No Acórdão Big Brother Watch e Outros c. Reino Unido, em que estava em causa a apreciação da compatibilidade da interceção massiva (e, como tal, generalizada e indiferenciada) de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego (*bulk interception*)[222] com o art. 8.º da CEDH, o TEDH, pese embora tenha condenado o Reino Unido, considerou que:

---

[219] Cfr. Acórdão da RC de 12/10/2022.

[220] Acolhido nos Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

[221] Nos termos previstos no art. 189.º, n.º 2, do CPP e na Lei n.º 109/2009, de 15 de setembro.

[222] Esta interceção massiva de dados de conteúdo e de dados de tráfego consiste em intercetar e recolher, de forma massiva, nos cabos óticos utilizados para a realização de comunicações, os dados relativos a todas as comunicações eletrónicas (incluindo os dados de conteúdo) realizadas por todos os dispositivos conectados a uma determinada rede de comunicações. A interceção massiva de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego passa por 4 fases:

Interceção e conservação dos dados informáticos relativos ao conteúdo de comunicações eletrónicas (dados de conteúdo) e dos dados relativos a comunicações (dados de tráfego);

Tratamento e seleção, de forma automatizada e com utilização de critérios de seleção, dos dados de conteúdo e de tráfego previamente conservados;

Exame, por analistas, dos dados de conteúdo e de tráfego previamente selecionados; e

a) A interceção massiva (e, como tal, generalizada e indiferenciada) de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego (*bulk interception*), por si só, não viola o art. 8.º da CEDH, contanto que sejam observadas determinadas garantias mínimas;
b) No caso da vigilância generalizada e indiferenciada (e que, por isso, não tem alvos determinados e delimitados), como é o caso da interceção massiva de dados de conteúdo e de dados de tráfego, as salvaguardas são ainda mais essenciais do que no caso da vigilância seletiva dirigida a pessoas determinadas (*targeted interception*);
c) Na medida em que a interceção massiva de dados de conteúdo e de dados de tráfego, pela sua própria natureza, é, por um lado, preventiva e prévia à existência de qualquer *notitia criminis* ou ao conhecimento da existência de uma ameaça concreta à segurança nacional e, por outro lado, generalizada e indiferenciada, não é possível aplicar-lhe duas das seis salvaguardas mínimas exigidas pelo TEDH no seu *case law* relativo às medidas de vigilância seletivas (*v.g.*, as escutas telefónicas): delimitação, pelo legislador, de um catálogo de crimes e de alvos e existência de uma suspeita fundada da prática de um crime do catálogo;
d) no entanto, ainda assim terão de ser existir salvaguardas mínimas no Direito interno dos Estados para que a interceção massiva de dados de conteúdo e de dados de tráfego observe as exigências do art. 8.º da CEDH, mais concretamente:

Conservação dos dados considerados relevantes após o respetivo exame e utilização desses dados, incluindo no que tange à sua partilha com outras entidades (nacionais ou estrangeiras).

No caso decidido pelo TEDH no citado aresto, as autoridades inglesas procediam à recolha, de forma massiva, para fins de segurança nacional, de todos os dados de conteúdo e dados de tráfego de todas as comunicações realizadas; subsequentemente, os dados obtidos eram sujeitos a um processo de seleção automatizado, com utilização de inteligência artificial, baseado em critérios abstratos de seleção, sendo destruídos os dados que não fossem considerados passíveis de possuírem relevância; seguidamente, os dados considerados como passíveis de possuírem relevância eram alvo de um segundo processo de seleção, agora manual, levada a cabo por analistas, sendo destruídos os dados que fossem considerados irrelevantes; e, por fim, os dados que haviam considerados pelos analistas como podendo possuir relevância eram alvo de conservação para ulterior utilização, sendo destruídos automaticamente ao fim de alguns meses.

- O Direito interno deverá prever, de forma clara, as circunstâncias em que as autoridades poderão lançar mão da interceção massiva de dados de conteúdo e de dados de tráfego, a duração da execução da medida, o procedimento relativo ao exame, utilização e conservação dos dados recolhidos, as precauções a observar relativamente à transmissão dos dados a outras entidades e em que circunstâncias os dados deverão ser apagados ou destruídos;
- Em face do carácter necessariamente secreto da interceção massiva de dados de conteúdo e de dados de tráfego (sob pena de inutilidade), a supervisão e o controlo efetivos (por uma entidade independente do poder executivo, que não é forçoso que seja um Juiz) da implementação da medida em todas as fases suprarreferidas (e não apenas relativamente à autorização do recurso à medida e à sua renovação) é absolutamente essencial para evitar abusos, incluindo no que tange à necessidade e à proporcionalidade do recurso à interceção em massa no caso concreto;
- O Direito interno deverá prever mecanismos que permitam às pessoas que suspeitem de que os seus dados foram alvo de interceção em massa contestar, de forma efetiva e não meramente aparente, a legalidade da medida e/ou a compatibilidade do regime da interceção em massa com a CEDH, sem dependência de qualquer notificação de que os seus dados foram alvo da medida; para tal, a entidade competente para apreciar a impugnação deverá ser independente do poder executivo (mas não tendo de ser necessariamente um Tribunal) e o procedimento terá de ser equitativo, devendo incluir a possibilidade de contraditório (na medida do possível) e a fundamentação da decisão, que deverá ser juridicamente vinculativa para o poder executivo, ao ponto de poder determinar a cessação de uma interceção ilegal e a destruição dos dados obtidos ou conservados de forma ilegal.

O TEDH também tem entendido que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (no sentido de serem utilizados meios de investigação que se mostrem necessários

para investigar no caso concreto) em ordem a investigar os crimes que atinjam algum dos direitos fundamentais garantidos pela CEDH, desde logo, no caso de homicídios, tendo em conta o disposto no art. 2.º da CEDH[223].

No que concerne à obtenção de metadados em investigações criminais, o TEDH considera que a não obtenção de metadados cuja obtenção se mostre necessária para uma determinada investigação criminal de crimes cometidos através da Internet ou com utilização da Internet é incompatível com o art. 8.º da CEDH (que também inclui um dever positivo de as autoridades levarem a cabo uma investigação efetiva e eficaz relativamente a crimes que lesem os direitos fundamentais tutelados por esse preceito da CEDH) se essa não obtenção puser em causa a eficácia dessa mesma investigação[224].

De resto, no Acórdão K.U. c. Finlândia é particularmente evidente a censura do TEDH à excessiva importância que foi atribuída pelas autoridades finlandesas à confidencialidade dos dados de tráfego dos internautas na investigação de uma situação em que um determinado indivíduo publicou um anúncio na Internet, levando a que um menor fosse alvo de abordagens de pedófilos; a Lei finlandesa em vigor, que visava proteger a liberdade de expressão e o direito à expressão anónima e protegia os autores de mensagens anónimas na Internet, impediu as autoridades de ordenarem ao fornecedor de serviços que lhes disponibilizasse metadados que permitissem a identificação do agente da infração, o que votara ao insucesso a investigação.

5. O Tratado da União Europeia e a Carta dos Direitos Fundamentais da União Europeia *vs.* a Convenção Europeia dos Direitos Humanos e a Constituição da República Portuguesa

Tanto o Acórdão Digital Rights do TJUE como o Acórdão do TC n.º 268/2002 incorrem numa falha grave, que se traduz na consideração apenas dos direitos fundamentais consagrados nos arts. 7.º e 8.º da CDFUE e 20.º, n.º 1, 26.º, n.º 1, e 35.º, n.ºs 1 e 4, da CRP.

---

223 Cfr. Acórdãos McCann e Outros c. Reino Unido, Mahmut Kaya c. Turquia, Hugh Jordan c. Reino Unido, Paul e Audrey Edwards c. Reino Unido, Nachova e Outros c. Bulgária, Kaya e Outros c. Turquia, Ramsahai e Outros c. Países Baixos, Angelova e Iliev c. Bulgária, Opuz c. Turquia, Kolevi c. Bulgária, Al-Skeini e Outros c. Reino Unido, Vasîlka c. Moldávia, Jaloud c. Países Baixos, Mustafa Tunç e Fecire Tunç c. Turquia e Armani da Silva c. Reino Unido.

224 Cfr. Acórdãos K.U. c. Finlândia, Khadija Ismayilova c. Azerbaijão e Volodina c. Rússia (n.º 2).

Todavia, existem outros direitos fundamentais protegidos pela CDFUE[225] que foram, pura e simplesmente ignorados pelo TJUE, sendo certo que a ponderação de interesses à luz do princípio da proporcionalidade tem de considerar *todos* os interesses contrapostos, precisamente porque essa ponderação visa obter uma concordância prática entre esses mesmos interesses. Além disso, o princípio da proporcionalidade foi considerado apenas na sua vertente de proibição do excesso, ignorando-se a vertente de proibição de insuficiência desse mesmo princípio[226], sobretudo quando está em causa, entre outras finalidades, "a luta contra a criminalidade grave"[227].

E o TC incorreu na mesma falha, ao também não considerar minimamente (ou se o considerou, tal não resulta do texto do Acórdão n.º 268/2022) os interesses (obviamente legítimos) prosseguidos por via da administração da Justiça penal (onde se inclui a investigação criminal e mesmo a prevenção criminal *ante delictum*), que visam a proteção dos direitos fundamentais dos cidadãos[228] contra o crime e

---

[225] De facto, a CDFUE também garante, no seu art. 6.º, os direitos à liberdade e à segurança, bem como, noutros preceitos, diversos direitos fundamentais que constituem o referente constitucional de bens jurídicos tutelados por diversos tipos de crime particularmente graves e cuja prevenção e repressão são essenciais num Estado de Direito, como, por exemplo, os direitos à vida (art. 2.º), à integridade pessoal (art. 3.º), a não ser escravizado nem alvo de redução à servidão ou sujeito a tráfico de seres humanos (art. 5.º), à propriedade (art. 17.º), à saúde (art. 35.º), ao ambiente (art. 37.º), a uma boa Administração (art. 41.º), à ação e a um Tribunal imparcial (art. 47.º), etc., que, na nossa ótica, não foram tidos em conta pelo TJUE. E o mesmo sucede, inclusivamente, com os direitos ao respeito pela vida privada e familiar (art. 7.º) e à proteção de dados pessoais (art. 8.º), que também podem ser lesados por via da prática de crimes, pelo que não podem ser considerados apenas para justificar a limitação da utilização de medidas de investigação criminal.

[226] Acerca do princípio da proporcionalidade na vertente de proibição de insuficiência e da sua aplicação no âmbito do Direito penal e processual penal, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 311 e ss.

[227] A que podemos subsumir a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta e outras formas de criminalidade, como os crimes sexuais (mesmo quando não impliquem o uso de violência e não sejam cometidos para obtenção financiamento do terrorismo e/ou de lucro para grupos criminosos organizados) ou mesmo os crimes puníveis com pena de prisão cujo limite máximo seja superior a 5 anos.

[228] De resto, o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, inclui crimes gravíssimos, como sejam: homicídio doloso, ofensa à integridade física grave, mutilação genital feminina, ofensa à integridade física agravada pelo resultado, violência doméstica, violação, coação sexual, abuso sexual de menores, roubo, extorsão, associação criminosa, tráfico de órgãos, tráfico de pessoas, tráfico de armas, tráfico de droga, corrupção, tráfico de influência, participação económica em negócio, branqueamento de capitais, grupo terrorista, terrorismo, financiamento do terrorismo, rapto, sequestro agravado, tomada de reféns,

não o engrandecimento do Estado[229]. E, como sabemos, para que a criminalização de uma conduta seja admissível, terá de estar em causa a proteção de um bem jurídico essencial à convivência comunitária e ao livre desenvolvimento da pessoa, que terá de estar relacionado com um direito fundamental ou com um interesse constitucionalmente protegido, sendo os bens jurídico-penais concretizações dos valores constitucionais expressa ou implicitamente ligados aos direitos e deveres fundamentais e à ordenação social, política e económica[230]; deste modo, no caso dos crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, está em causa a proteção de alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional[231].

Ainda no que tange à CDFUE, há que ter em conta o disposto no seu art. 53.º, nos termos do qual, «*Nenhuma disposição da presente Carta deve ser interpretada no sentido de restringir ou lesar os direitos do Homem e as liberdades fundamentais reconhecidos, nos respetivos âmbitos de aplicação, pelo direito da União, o direito internacional e as Convenções internacionais em que são Partes a União ou todos os Estados-Membros, nomeadamente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, bem como pelas Constituições dos Estados-Membros*».

Daqui resulta que a aplicação da CDFUE não pode conduzir a uma menor proteção de direitos fundamentais do que a proteção proporcionada por outros instrumentos de Direito internacional (como a CEDH) ou das Constituições dos Estados-Membros.

No caso da CRP, cumpre considerar o art. 8.º, n.º 4, nos termos do qual, as normas do Direito da União Europeia são aplicáveis na ordem jurídica portuguesa nos termos definidos pelo Direito da União Europeia (incluindo a sua interpretação

---

escravidão, tortura, etc. De todo o modo, afigura-se-nos que este catálogo é excessivamente restritivo, não se percebendo, desde logo, porque é que é mais restritivo do que o catálogo dos arts. 187.º, n.º 1, do CP e 18.º, n.º 1, da Lei n.º 109/2009.

[229] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 1, p. 147.

[230] Cfr. FIGUEIREDO DIAS, Direito Penal, Parte Geral, Tomo I, 3.ª Edição, pp. 136 e ss., e DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, p. 88.

[231] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 33.

pelo TJUE), *mas sempre com respeito pelos princípios fundamentais do Estado de Direito Democrático*, sendo que esta reserva constitucional prevista na parte final do n.º 4 do art 8.º da CRP, nas palavras de GOMES CANOTILHO/VITAL MOREIRA[232], «*poderá considerar-se como uma norma de colisão explícita, pois ela torna claro que o princípio do primado do direito da União está limitado por núcleo essencial da Constituição – princípios fundamentais do Estado de direito democrático – que funcionarão como uma espécie de «reserva de ordem pública constitucional» («teoria dos contratualistas») contra eventuais preceitos ou disposições do direito da União aniquiladores da estadualidade (Estado), juridicidade (Estado de direito), democraticidade (Estado de direito constitucional) e fundamentalidade de direitos básicos (Estado de direitos fundamentais)*».

No fundo, esta reserva constitucional do art. 8.º, n.º 4, *in fine*, da CRP corresponde *grosso modo* à ressalva contida no art. 53.º da CDFUE.

Ainda no que concerne ao Direito da União Europeia, nos termos do art. 6.º, n.º 2 e 3, da CDFUE (na versão *oficial* portuguesa):

«*2. A União adere à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essa adesão não altera as competências da União, tal como definidas nos Tratados.*

3. Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros».

Ainda que, formalmente, a UE não tenha aderido à CEDH e, pelo menos, as versões inglesa e espanhola refiram que a UE "aderirá" e que os direitos fundamentais garantidos pela CEDH "farão parte" do Direito da União Europeia enquanto princípios gerais de direito, pelo menos nas versões portuguesa, italiana, alemã e francesa, refere-se que a UE "adere" e que os direitos fundamentais garantidos pela CEDH "fazem parte" do Direito da União Europeia enquanto princípios gerais de direito. Por isso, do ponto de vista material, tendo em conta, não apenas o art. 6.º, n.ºs 2 e 3, do TUE, mas sobretudo o art. 53.º da CDFUE, a UE, do ponto de vista material, está vinculada à CEDH e os direitos fundamentais garantidos pela CEDH tal como interpretados pelo TEDH integram o Direito da União Europeia. E não podemos olvidar

[232] GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, p. 267.

que os Estados-Membros da UE são igualmente Estados-Membros do Conselho da Europa, estando, por isso, sujeitos à CEDH e à jurisprudência do TEDH.

Deste modo, a CEDH, tal como interpretada pelo TEDH, prevalece sobre a CDFUE e a jurisprudência do TJUE[233], que cedem igualmente perante a CRP nos casos em que esta conceda uma melhor proteção dos direitos fundamentais[234], sendo que a prevenção e a repressão de crimes graves são justificadas e mesmo impostas, no plano jurídico-constitucional, enquanto mecanismos de proteção dos bens jurídico-penais e, consequentemente, de direitos fundamentais[235].

E, como referimos, o TEDH considera que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (o que inclui a obrigação de utilizar os meios de investigação que, não violando o disposto na CEDH, se mostrem necessários no caso concreto) dos crimes que lesem ou ponham em perigo algum dos direitos fundamentais garantidos pela CEDH, não faltando casos de condenação de Estados por ineficácia da investigação criminal em virtude do não uso de meios investigatórios que se mostrem necessários para investigar os crimes em causa no caso concreto.

6. Apreciação crítica da jurisprudência do Tribunal de Justiça da União Europeia e do Tribunal Constitucional em matéria de conservação e utilização de metadados conservados na investigação criminal

Compulsados os textos dos Acórdãos Digital Rights (do TJUE) e n.º 268/2022 (do TC), deparamos, desde logo, com uma grave falha metodológica, que se prende com o facto de, em ambos os arestos, não ter sido realizada qualquer

233 Como resulta dos arts. 6.º, n.ºs 2 e 3, do TUE e 53.º da CDFUE.

234 Cfr. arts. 53.º da CDFUE e 8.º, n.º 4, *in fine*, da CRP.

235 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 334 e ss. (sobretudo na p. 336), e voto de vencido do Juiz Schluckebier na Sentença do BVerfG de 02/03/2010.

E, como referimos, os crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 protegem alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional (cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 33).

ponderação entre os direitos à intimidade/privacidade e à autodeterminação informacional (ambos os Tribunais) e à tutela jurisdicional efetiva (no caso do TC) e os direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (no caso do TC) e pelos crimes subsumíveis ao conceito de criminalidade grave[236] utilizado pelo TJUE (no caso do TJUE)[237].

Contudo, dado que, do outro lado da rua, também está em causa a proteção de direitos fundamentais, impunha-se que o TJUE e o TC tivessem realizado uma ponderação entre os interesses em conflito, não se podendo olvidar que alguns dos direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e pelos crimes subsumíveis ao conceito de criminalidade grave integram o elenco dos direitos fundamentais mais relevantes à luz da ordem de valores jurídico-constitucional da CRP e da CDFUE e que direitos como o direito à vida e à integridade pessoal são, inclusivamente, mais valiosos dos que os direitos invocados pelo TJUE para invalidar a Diretiva 2006/24/CE e pelo TC para declarar a inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 109/2009.

Além disso, a ponderação teria sempre de ser levada a cabo *in concreto* (ou seja, considerando a natureza, o âmbito e a intensidade da restrição dos direitos à intimidade/privacidade, à autodeterminação informacional e à tutela jurisdicional efetiva) e não em abstrato (com base numa ideia de ordem hierárquica de valores constitucionais)[238], sendo que, como veremos, as restrições a estes direitos por via da

---

[236] A que podemos subsumir a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta e outras formas de criminalidade, como os crimes sexuais (mesmo quando não impliquem o uso de violência e não sejam cometidos para obtenção financiamento do terrorismo e/ou de lucro para grupos criminosos organizados) ou mesmo os crimes puníveis com pena de prisão cujo limite máximo seja superior a 5 anos.

[237] A nossa apreciação cinge-se à questão do combate à criminalidade, que inclui a segurança pública (que é a questão que foi tida em conta pelo TC no Acórdão n.º 268/2022), não se considerando a questão da admissibilidade da obtenção de metadados pelos serviços de informações para salvaguarda da segurança nacional (que também tem sido considerada na jurisprudência do TJUE e foi objeto dos Acórdãos do TC n.ºs 403/2015 e 464/2019, em que o TC considerou, e bem, inconstitucionais, normas que previam o acesso, pelos serviços de informações a metadados).

[238] Cfr. VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 323, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos

conservação e utilização probatória de metadados conservados, nos casos em que existem efetivamente, são de intensidade pouco significativa.

Não obstante, o TJUE e o TC não realizaram qualquer ponderação de interesses, afigurando-se-nos que, se essa ponderação tivesse sido realizada, o TC jamais teria declarado a inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 109/2009.

Na sua jurisprudência subsequente ao Acórdão Digital Rights (relativa à Diretiva 2002/58/CE, conforme alterada pela Diretiva 2009/136/CE)[239], o TJUE passou a fundamentar as decisões numa ponderação de interesses, tendo enunciado os seguintes parâmetros:

a) A CDFUE proíbe a conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica;
b) A CDFUE impõe que os dados sejam conservados no território da União Europeia;
c) A CDFUE permite a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave, real e atual ou previsível[240], desde que essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça, e a decisão que determina a conservação seja efetivamente fiscalizada por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos;

"ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 310.

[239] Cfr. Acórdãos Tele2 Sverige AB e Secretary of State for the Home Department, Ministerio Fiscal, Privacy International, La Quadrature du Net, Prokuratuur, G. D. e Commissioner of An Garda Síochána e SpaceNet e Telekom Deutschland.

[240] O que, no caso de Portugal, torna impossível a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, sendo certo que o TJUE apenas admite esta conservação generalizada e indiferenciada para fins de salvaguarda da segurança nacional e não para fins de resposta à criminalidade grave (ainda que algumas formas de criminalidade grave sejam, concomitantemente, ameaças à segurança nacional, como sucede com o terrorismo), o que não se entende.

d) A CDFUE permite a conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;
e) A CDFUE permite conservação generalizada e indiferenciada, por um período temporalmente limitado ao estritamente necessário, dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional;
f) A CDFUE permite conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública; e
g) A CDFUE permite o acesso a metadados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (que não inclui o MP, pois é o titular da ação penal).

O que dizer destas condições impostas pelo TJUE?

Em primeiro lugar, no caso da conservação seletiva, as condições são impossíveis de cumprir e são de difícil (ou mesmo impossível) determinação.

São impossíveis de cumprir porque a conservação de metadados é uma medida de prevenção criminal que se integra na chamada investigação proativa e ocorre, por natureza, num momento prévio à obtenção da notícia do crime, sendo, por isso, *impossível* definir um qualquer critério delimitador dos metadados a conservar e, ainda que fosse possível, tal critério sempre violaria os princípios da proibição da discriminação e da presunção de inocência.

São de difícil (ou mesmo impossível) determinação, pois, ainda que o TJUE esclareça que a preservação da segurança nacional corresponde ao interesse

primordial de proteger as funções essenciais do Estado e os interesses fundamentais da Sociedade, através da prevenção e da repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país (em especial, ameaçar diretamente a Sociedade, a população ou o Estado), dando o exemplo do terrorismo, fica por saber, por exemplo, se tal também inclui a criminalidade organizada (*maxime* as máfias) e, na afirmativa, se inclui todos os casos de criminalidade organizada mafiosa ou apenas aqueles casos em que as máfias ameacem diretamente o Estado, os seus agentes e os cidadãos de uma forma generalizada (gerando um ambiente generalizado de medo), excluindo as situações em que isso não suceda ou tenha deixado de suceder.

E são de difícil (ou mesmo impossível) determinação também pelo facto de não vermos como é que, com base em elementos objetivos e não discriminatórios (e quais são ou poderão ser esses elementos), em função das categorias de pessoas em causa ou através de um critério geográfico, será possível definir um qualquer critério delimitador dos metadados a conservar e, sobretudo, fazê-lo sem violar a presunção de inocência e a proibição de discriminação.

Podemos, pois, afirmar, com segurança, que a conservação seletiva dos dados de tráfego e dos dados de localização nos termos propostos pelo TJUE é absolutamente inviável e, por isso, esta (aparente) possibilidade é, na realidade, uma impossibilidade.

Em segundo lugar, na sequência do que referimos, estas exigências abrem a porta a um tratamento discriminatório entre os cidadãos, pois a limitação da conservação de dados em função das categorias de pessoas (*v.g.*, indivíduos com antecedentes criminais ou com antecedentes criminais de uma determinada tipologia, indivíduos oriundos de países ou de regiões conotadas com determinadas atividades criminosas ou que desempenham uma determinada atividade profissional ou económica conotada com certas atividades criminosas) ou de um critério geográfico (*v.g.*, os habitantes de uma determinada região, de uma determinada localidade, de parte de uma localidade ou de um bairro) encerra um enorme risco de discriminação dos visados face aos não visados, inclusivamente no que tange à presunção de inocência e não apenas no que concerne ao tratamento informático de dados relativos à vida privada *ex se*.

Em terceiro lugar, o entendimento do TJUE ignora o facto de a criminalidade organizada, o terrorismo, o cibercrime e a criminalidade económico-financeira serem formas de criminalidade tendencialmente e em muitos casos (porventura na maioria dos casos) transnacional, podendo a atividade criminosa desenvolver-se no território de dois ou mais Estados; e alguns dos Estados em que atividade criminosa é levada a cabo poderão ser Estados não-membros da UE (e, como tal, não sujeitos à jurisprudência do TJUE), mas aos quais o ou os Estados-Membros da UE deva(m) prestar cooperação no âmbito de instrumentos de Direito internacional extracomunitários (*v.g.*, instrumentos de prevenção e repressão da criminalidade adotados no âmbito da ONU ou do Conselho da Europa[241]).

Em quarto lugar, o TJUE também olvida que a atividade criminosa pode ser levada a cabo ou as suas consequências danosas podem verificar-se no Estado A, mas os criminosos utilizarem o Estado B como base de operações ou como ponto de recuo depois do cometimento dos crimes ou praticarem no Estado B os atos preparatórios ou de execução dos crimes cujas consequências se verificam no Estado A; e também olvida que as ações de prevenção criminal relativamente a crimes que virão ou poderão vir a ser cometidos no Estado A podem ter de ser levadas a cabo também no Estado B.

Em quinto lugar, relativamente aos casos em que o TJUE admite a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, não se percebe como é que tal só é admitido para fins de salvaguarda da segurança nacional (ou seja, pelos serviços de informações) e não também para a luta contra a criminalidade grave (ainda que algumas formas de criminalidade grave sejam, concomitantemente, ameaças à segurança nacional, como sucede com o terrorismo).

E, em sexto lugar, relativamente à diferenciação entre os endereços IP atribuídos à fonte de uma ligação (que serão, tendencialmente, dados de base) e os dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (que também são dados de base), não se entende uma tal diferenciação, sobretudo quando, pelo menos à partida, em termos de privacidade, o conhecimento da residência de uma pessoa será mais lesivo do que o

241 Daí resultando que a jurisprudência do TJUE pode pôr em causa instrumentos de combate à criminalidade adotados no âmbito da ONU ou do Conselho da Europa.

conhecimento do IP que está atribuído a um determinado sistema informático e, apesar disso, o TJUE é bastante mais restritivo quanto à admissibilidade da conservação generalizada e indiferenciada dos os endereços IP do que quanto à admissibilidade da conservação generalizada e indiferenciada dos dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos.

Passando ao TC, tendo em conta o que já referimos e o que referiremos infra, o TC não estava obrigado a seguir a jurisprudência do TJUE no Acórdão Digital Rights. No entanto, o Acórdão do TC n.º 268/2022 padece de problemas muito mais graves do que a ausência de ponderação entre os direitos à intimidade/privacidade, à autodeterminação informacional e à tutela jurisdicional efetiva e os direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008.

Em primeiro lugar, ao contrário do que é afirmado pelo TC (e aqui divergimos do voto de vencido) e pelo TJUE, a mera conservação de metadados não restringe qualquer direito fundamental[242], apenas ocorrendo uma restrição se e quando os

[242] Dado que, nos termos dos arts. 3.º, n.º 3, e 7.º, n.º 2, da Lei n.º 32/2008, os metadados terão de ser guardados em ficheiros (*que têm de estar obrigatoriamente separados de quaisquer outros ficheiros para outros fins*) e *encriptados* e, nos termos dos arts. 3.º, n.ºs 1 e 2, 8.º e 9.º, n.º 1 (abstraindo do facto de considerarmos que este preceito foi tacitamente revogado pela Lei n.º 109/2009 (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 557 e ss., e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 65 e ss.), esses ficheiros só podem ser desencriptados e acedidos para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes e mediante despacho judicial fundamentado; isto sem embargo de, por entendermos que o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, a entidade competente para autorizar o acesso aos metadados seja a autoridade judiciária no caso de dados de base e de localização celular (cfr. art. 14.º, n.ºs 1 e 4, da Lei n.º 109/2009) e, no caso dos dados de tráfego, o JIC ou o Juiz (cfr. arts. 18.º, n.º 2, da Lei n.º 109/2009, na fase de inquérito, e 189.º, n.º 2, do CPP, nas demais fases processuais). Aliás, não vemos em que medida a obtenção de dados conservados terá de ser rodeada de maiores garantias do que no caso de esses dados serem obtidos em tempo real.

Além disso, só os funcionários do operador de comunicações eletrónicas que estejam especialmente autorizados para tal poderão aceder aos dados, sob pena de responsabilidade penal (cfr. art. 13.º, n.º 1, al. c), da Lei n.º 32/2008), e a sua identidade tem de ser comunicada à CNPD, sob pena de responsabilidade contraordenacional (cfr. art. 12.º, n.º 1, al. d), da Lei n.º 32/2008).

Ou seja, na fase de conservação, os metadados são, apenas e só, inseridos em ficheiros que ficavam encriptados e intocados até à sua destruição ao fim de 1 ano, a menos que fosse autorizado o acesso a determinados metadados (que seriam apenas os metadados relativos ao arguido, ao suspeito, ao intermediário ou, mediante consentimento, à vítima e não a todos os metadados que estivessem naquele ou naqueles ficheiros) e nada mais.

dados forem acedidos[243], sendo que a conservação, por si só, não revela quaisquer informações, apenas permitindo o uso futuro de elementos de prova em investigações criminais que, de outro modo, teriam desaparecido e não poderiam ser utilizados, num Estado de Direito, esse aumento da eficácia da investigação só pode ser considerado positivamente[244]. No fundo, tal como sucede na preservação expedita de dados informáticos e na revelação expedita de dados de tráfego previstas nos arts. 12.º e 13.º da Lei n.º 109/2009[245], a conservação de metadados não restringe qualquer direito fundamental.

Em segundo lugar, ainda que se admitisse que a mera conservação de metadados restringe direitos fundamentais, tratar-se-ia de uma restrição pouco intensa[246].

---

[243] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 28.

[244] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 29.

De resto, como vimos, o TEDH tem considerado que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (o que inclui a obrigação de utilizar os meios de investigação que, não violando o disposto na CEDH, se mostrem necessários no caso concreto) dos crimes que lesem ou ponham em perigo algum dos direitos fundamentais garantidos pela CEDH.

[245] Cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 84-84 e 101.

[246] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 30.

De resto, no que tange aos dados de base, o próprio TC, no Acórdão n.º 268/2022, considera que se trata de uma restrição pouco intensa.

No caso dos dados de localização, a única informação que esses dados fornecem é a localização de um determinado dispositivo, a partir da qual se vai *inferir* (de forma ilidível) que o seu proprietário ou utilizador habitual se encontra nesse mesmo local, sendo incorreto afirmar que os dados de localização permitem *saber* a localização de uma pessoa; por isso, a obtenção (e não a conservação, que não revela quaisquer dados) de dados de localização celular constitui uma restrição pouco intensa de direitos fundamentais (cfr. DUARTE RODRIGUES NUNES, "Da admissibilidade da obtenção de dados de localização celular ou de dados de tráfego de todos os telemóveis/cartões que acionaram um determinado conjunto de antenas/células de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado, para posterior identificação dos seus autores", *in* RMP, n.º 157, p. 133, Acórdãos do TC n.º 486/2009 e do STJ de 29/04/2010 e Sentenças do

Em terceiro lugar, a conservação e os ulteriores acesso e utilização de metadados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes (cfr. art. 3.º, n.º 1, da Lei n.º 32/2008), o que inclui a repressão criminal e a prevenção criminal, tendo em conta o *continuum* que existe (e terá de existir[247]) entre ambas como *conditio sine qua non* para responder eficazmente à criminalidade organizada, ao terrorismo, à criminalidade económico-financeira e ao cibercrime[248]. E, como referimos, o

BGH de 24/01/2001 e do *Tribunal Supremo* n.º 6307/2009; contra, Acórdão do TC n.º 268/2022 e Sentença United States v. Jones do *Supreme Court of the United States*).

Por fim, no caso dos dados de tráfego, trata-se dos elementos ou dados funcionais necessários ou produzidos pelo estabelecimento da ligação através da qual uma comunicação concreta é operada ou transmitida [a direção, o destino (*adressage*) e a via, o trajeto (*routage*)], os quais se limitam a revelar – no caso de comunicações telefónicas – os números das chamadas recebidas e os números para os quais aquele dispositivo ligou (daí se *inferindo*, uma vez mais de forma ilidível, que as comunicações tiveram lugar entre os proprietários ou os utilizadores habituais de cada um desses números telefónicos) e a data, a duração, a hora, e a frequência dessas comunicações ou tentativas de comunicação e nada mais, pois nada revelam quanto ao conteúdo das comunicações; por isso, trata-se de uma restrição também pouco intensa de direitos fundamentais e que, por ser muito menos intensa do que no caso da obtenção de dados de conteúdo, a sua obtenção, ainda que restrinja o direito à inviolabilidade das comunicações, nem deveria estar sujeita ao regime particularmente restritivo das interceções de comunicações (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 577), como sucede no Direito alemão (em que o legislador consagrou, no §100g da StPO, um regime muito menos restritivo do que o das interceções de comunicações do §100a).

Reconhecemos, porém, que a intensidade da restrição poderá ser mais intensa – embora sem que possa ser comparada à obtenção de dados de conteúdo de comunicações por via da interceção de comunicações – no caso dos dados de tráfego relativos à navegação na Internet, ainda que, também aqui, apenas se obtenham as informações relativas às páginas de Internet "visitadas" por via daquele sistema informático, inferindo-se, a partir daí (de forma ilidível), que foi o proprietário ou utilizador habitual desse sistema informático quem acedeu a essas páginas (e, por isso, a restrição também não pode ser qualificada como intensa).

[247] Sobre esse *continuum*, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 255 e ss.

[248] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 581, e também em "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 32.

catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008[249] inclui crimes gravíssimos, cujos bens jurídicos protegidos têm como referente constitucional alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional.

Ora, a utilização de metadados tende a ser absolutamente essencial para muitas investigações criminais desses tipos de crime (e de outros), *maxime* quando se trate de formas de criminalidade que utilizam sistematicamente meios informáticos e/ou outros meios eletrónicos de comunicação à distância (designadamente, a criminalidade organizada, o terrorismo, a criminalidade económico-financeira ou o cibercrime[250] *ex se*) cuja utilização gera metadados[251]. E, como é óbvio, a notícia do crime é sempre obtida após a prática do crime (e, não poucas vezes, muito depois) e, mesmo quando o processo é instaurado pouco tempo após a prática do crime, muitas vezes, a identificação de arguidos ou suspeitos só ocorre muito tempo depois da instauração do processo (e só aí é que a obtenção de metadados relativos ao suspeito, ao arguido ou ao intermediário será possível e admissível)[252]. Por isso, os metadados que interessa obter são metadados gerados no passado e não no decurso da investigação, sendo essa situação que o legislador pretendeu acautelar ao impor a conservação dos metadados através da Lei n.º 32/2008 e o mesmo

[249] Embora consideremos que a obtenção de dados de localização ou de base não está sujeita a qualquer catálogo de crimes (cfr. art. 14.º da Lei n.º 109/2009) e que a obtenção de dados de tráfego está sujeita ao catálogo do art. 18.º, n.º 1, da Lei n.º 109/2009, que é mais amplo do que o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008.

[250] Que, quando entendido em sentido lato (tal como defendemos), inclui tanto os crimes em que o sistema informático ou os dados informáticos são o objeto da ação, ainda que como alvos simbólicos (cibercrime em sentido estrito) como outros crimes cujo cometimento esteja significativamente ligado à utilização de um sistema informático (onde se incluem, por exemplo, a pornografia infantil, a extorsão sexual, o tráfico de drogas ou armas, o jogo ilícito *online*, as burlas relativas a criptomoedas, etc.) (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 45-46).

[251] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 33-34.

[252] Assim, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 34.

sucedendo com o Parlamento Europeu e o Conselho ao adotarem a Diretiva 2006/24/CE[253].

Tendo em conta o que acabámos de referir, além de a mera conservação de metadados não restringir direitos fundamentais e de o acesso aos metadados apenas constituir uma restrição de direitos fundamentais que não pode ser considerada intensa, a desconsideração[254] da necessidade de investigar eficazmente os crimes graves constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 configura uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais tutelados por esses crimes[255], sendo que a Lei n.º 32/2008 encontrara um equilíbrio que proporcionava uma muito adequada concordância prática entre os valores em colisão[256]. Aliás, atentas a natureza dos crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, a intensidade da restrição de direitos fundamentais que o acesso e a utilização dos metadados acarretam e as salvaguardas que o legislador previra na Lei n.º 32/2008, os direitos ou interesses constitucionalmente protegidos prosseguidos através da investigação criminal tendem a ser mais relevantes à luz da ordem de valores jurídico-constitucional do que os direitos fundamentais restringidos, o que foi completamente ignorado pelo TC[257]. E não podemos olvidar que o interesse público numa Justiça penal funcionalmente eficaz é um pressuposto essencial do Estado de Direito e

253 Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 34.

254 Ao ponto de ocorrer um sacrifício a cem por cento do valor da segurança (cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 34, e voto de vencido do Acórdão do TC n.º 268/2022) e dos demais direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (cfr. DUARTE RODRIGUES NUNES, *Idem*, pp. 34-35).

255 Como resulta da jurisprudência do TEDH que referimos.

256 Como se aduz no voto de vencido do Acórdão do TC n.º 268/2022.

257 Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 35.

possui, também ele, respaldo constitucional[258], sendo que a investigação dos crimes e a punição dos criminosos é levada a cabo em prol do interesse da Comunidade no seu todo e não em prol do engrandecimento do Estado[259].

Em quarto lugar, como se afirma no voto de vencido, se só for possível conservar metadados relativamente a pessoas em relação às quais existam indícios de que o seu comportamento possa ter algum nexo com os crimes graves enunciados na al. g) do n.º 1 do art. 2.º da Lei n.º 32/2008, os fornecedores de serviços de telecomunicações apenas poderão conservar os dados quando a autoridade judiciária competente os solicitar no decurso de uma investigação criminal, situação que já está prevista no art. 12.º da Lei n.º 109/2009 (cuja aplicação depende de os dados a preservar terem sido previamente conservados[260]), mas que poderá ser insuficiente para o apuramento da verdade e para a efetiva recolha de prova[261].

Em quinto lugar, apesar de a Lei n.º 32/2008 ser o diploma através do qual o legislador transpôs a Diretiva 2006/24/CE para o Direito português, a declaração de invalidade da Diretiva não implica por si só a invalidade da Lei n.º 32/2008 à luz do Direito União Europeia, pois a conservação e a obtenção de registos da realização

---

[258] Cfr. FIGUEIREDO DIAS, Acordos Sobre a Sentença em Processo Penal, pp. 37 e ss., DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 335 e ss., e também em Curso de Direito Processual Penal, 1, p. 147, CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* RMP, n.º 139, p. 39 (nota 21), Acórdãos Paul e Audrey Edwards c. Reino Unido do TEDH, do TC n.º 213/2008, do STJ de 03/03/2010 e da RL de 24/01/2012 e Sentenças do BVerfG de 27/06/2018, National City Trading Corp. *v.* United States do *United States Court of Appeals, 2nd Circuit* (1980) e **United States *v.* Hunter** do *United States District Court, Vermont* (1998).

[259] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 35.

[260] No mesmo sentido, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 36 (nota 38), e RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, p. 38.

[261] Por exemplo, numa situação de rapto, se os dados relativos às comunicações das vítimas não forem conservados, poderá ser muito difícil identificar os agentes dos crimes, uma vez que os metadados que vierem a ser obtidos em tempo real serão tendencialmente inúteis, dado que os telefones das vítimas terão sido certamente deixados no local onde o rapto ocorreu, para impedir a sua monitorização pelas autoridades.

de comunicações e de dados de localização não dependem, *ex se*, dessa Diretiva, nada impedindo a sua consagração legal na falta de uma tal Diretiva[262]. Ademais, o legislador nacional criou um quadro normativo que vai muito para além da Diretiva ao prever um regime jurídico que cumpre as exigências cuja inobservância pela Diretiva levou o TJUE a declarar a invalidade da Diretiva não sejam aplicáveis à Lei n.º 32/2008[263].

Em sexto lugar, permitindo a Lei que os prestadores de serviços de comunicações eletrónicas conservem, pelo prazo de seis meses, uma grande parte dos metadados incluídos no art. 4.º da Lei n.º 32/2008 para efeitos de faturação (cfr. arts. 6.º, n.º 3, e 7.º da Lei 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho)[264], não se pode conceber que o interesse privado das operadoras cobrarem os serviços prestados aos seus clientes possa ser mais relevante do que o interesse público numa Justiça penal funcionalmente eficaz, sobretudo quando se trate da investigação de crimes que atentam contra os valores mais eminentes da ordem de valores jurídico-constitucional (como sucede com a vida e/ou a integridade pessoal, que a CRP reputa como invioláveis), ao ponto de se admitir como constitucionalmente admissível a conservação de dados para efeitos de faturação e o mesmo já não suceder no caso de conservação para fins de investigação criminal[265].

Em sétimo lugar, no que diz respeito à não previsão da obrigatoriedade de os dados serem conservados num Estado-Membro da União Europeia, como se aduz

---

[262] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 559.

[263] Relativamente às razões porque entendemos que os fundamentos que levaram o TJUE a declarar a invalidade da Diretiva não são aplicáveis à Lei n.º 32/2008, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 559 e ss.

[264] E sem que isso ponha em causa a privacidade dos utilizadores, ao ponto de não ter sido também peticionada a declaração da inconstitucionalidade das normas que permitem a conservação para efeitos de faturação, ao contrário do que sucedeu relativamente aos arts. 4.º e 6.º da Lei n.º 32/2008.

[265] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", *in* Comentário do Código de Processo Penal, Vol. I, 5.ª Edição, pp. 859-860, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 39, e voto de vencido no Acórdão n.º 268/2022.

no voto de vencido, é um problema que nem sequer se deveria colocar, pois o art. 7.º, n.º 4, da Lei n.º 32/2008 remete para as Leis n.ºs 67/98, de 26 de outubro (sendo que, atualmente, a questão está regulada nos arts. 44.º e ss. do RGPD), e 41/2004, de 18 de agosto, onde se resolve a questão da territorialidade e da transferência dentro e para fora da União Europeia (o que torna desnecessária a repetição dessa regulação na Lei n.º 32/2008) e, além disso, quando a Lei sujeita a conservação dos dados ao controlo da CNPD, está a impor, implicitamente, que os dados sejam conservados no território português[266].

Em oitavo lugar, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável, pelo que também a defesa (e não apenas a acusação) fica impossibilitada de utilizar tais provas, que também poderão impedir condenações insustentável e materialmente injustas[267].

Em nono lugar, no que diz respeito à não notificação dos titulares dos dados de que os seus dados foram acedidos pelas autoridades, na maioria das situações, essa notificação é desnecessária e redundante, dado que os dados que foram acedidos são os dados do arguido, que, tendo acesso aos autos, terá perfeito conhecimento de que os seus dados foram acedidos e poderá exercer os seus direitos a esse respeito. Além disso, como se refere no voto de vencido, o art. 9.º da Lei n.º 32/2008 nem sequer é o preceito em que a obrigação da notificação do titular dos dados acedidos deveria constar, pelo que declarar a inconstitucionalidade deste preceito com um tal fundamento não faz qualquer sentido. Ademais, é manifestamente excessivo e desrazoável declarar a inconstitucionalidade de uma norma e, com isso, vedar o recurso a um meio de obtenção de prova absolutamente essencial para investigar crimes graves (na medida em que permite a obtenção de

[266] DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 40.

[267] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 41.

um meio de prova essencial para essa finalidade[268]), com um tal fundamento, sobretudo tendo em conta as consequências jurídicas que poderão advir de uma tal decisão[269].

Em décimo lugar, o entendimento do TC (na esteira do jurisprudência do TJUE), ao poder comprometer seriamente (ou mesmo impossibilitar) muitas investigações criminais de crimes graves ou de formas de criminalidade extremamente danosas e perigosas para os direitos fundamentais dos cidadãos e para a própria subsistência do Estado de Direito – sendo, por isso, violador da CEDH –, poderá conduzir a condenações do Estado Português no TEDH e no pagamento de indemnizações às vítimas, por responsabilidade civil no exercício da função jurisdicional.

Em décimo primeiro lugar, o TC, ainda que reconhecendo que não é possível configurar medidas com a mesma eficácia que a conservação de todos os dados de todas as pessoas, considerou que a conservação de metadados só será legítima se, como entendeu o TJUE, for limitada a dados de localização e de tráfego relativos a um período temporal e/ou a uma zona geográfica determinada e/ou um círculo de pessoas determinado (*in casu*, pessoas que possam estar envolvidas de alguma forma numa infração grave e/ou pessoas que, por outros motivos, a conservação dos seus dados possa contribuir para a luta contra a criminalidade grave), o que levanta, desde logo, dois problemas.

O primeiro desses problemas (porventura o mais grave) é que a limitação da conservação de metadados em função de categorias de pessoas (*v.g.*, indivíduos com antecedentes criminais ou com antecedentes criminais de uma determinada tipologia, indivíduos oriundos de países ou de regiões conotadas com determinadas atividades criminosas ou que desempenham uma determinada atividade

---

[268] Como refere RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 34-35, os metadados são um meio de prova, *in casu*, documental (e não um meio de obtenção de prova), que «*podem estar inscritos numa factura detalhada que seja enviada por correio físico ou electrónico para o domicílio do seu titular; podem ser registados através de intercepção das comunicações telefónicas ou de dados informáticos (cf. infra); alguns podem ser encontrados nos sistemas informáticos utilizados nas comunicações; podem estar conservados pelos FS* [fornecedores desses serviços]».

[269] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 41.

profissional ou económica conotada com certas atividades criminosas) ou de um critério geográfico (*v.g.*, os habitantes de uma determinada região, de uma determinada localidade, de parte de uma localidade ou de um bairro) constitui um tratamento discriminatório. Na verdade, como se afirma no voto de vencido, a conservação preventiva de dados geograficamente condicionada, dirigida a um círculo de pessoas determinadas e sem qualquer facto típico cometido não é tolerada pela norma do n.º 3 do art. 35.º da CRP, que apenas admite que o legislador autorize o tratamento informático de dados relativos à vida privada «*com garantias de não discriminação*» e, por isso, o acolhimento, nesta parte, da jurisprudência do TJUE viola, inclusivamente o disposto nos arts. 8.º, n.º 4, *in fine*, da CRP e 53.º da CDFUE, residindo aqui o primeiro fundamento da inconstitucionalidade do próprio juízo de inconstitucionalidade formulado pelo TC no Acórdão n.º 268/2022.

Mas, esse juízo de inconstitucionalidade também viola o princípio da presunção de inocência, uma vez que a conservação preventiva de dados que vise apenas um círculo de pessoas determinadas e sem qualquer facto típico cometido, pela natureza das coisas, pressupõe uma suspeita de que aquele ou aqueles concretos visados poderão ter cometido ou vir a cometer crimes de que nem sequer existe notícia. E tal situação não tem comparação com a recolha de ADN (argumento que também é utilizado pelo TC), pois a recolha de ADN a condenados é uma consequência jurídica da condenação (que está, de resto, limitada aos casos de maior gravidade e/ou perigosidade[270]) e, ao passo que o ADN é imutável, o condenado pode sempre mudar de dispositivo (telefone, *tablet*, computador), de número de telefone ou de IP ou deixar de os utilizar para o cometimento de crimes (pois sabe que iriam ser monitorizados), tornando a conservação de dados de tráfego e de localização completamente inútil.

Ainda relativamente à presunção de inocência, nem se diga que a conservação generalizada e indiscriminada de metadados constitui uma presunção de culpa ou uma suspeita generalizada sobre todos os cidadãos, uma vez que,

[270] Pois a Lei exige que o visado tenha sido condenado com pena igual ou superior a 3 anos de prisão, ainda que substituída, ou alvo da aplicação de medida de segurança de internamento de inimputáveis, ainda que suspensa na sua execução (cfr. art. 8.º, n.ºs 2 e 3, da Lei n.º 5/2008, de 12 de fevereiro (acerca da obrigatoriedade e da automaticidade da recolha de ADN em arguidos condenados, *vide* DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "Artigo 172.º", *in* Comentário do Código de Processo Penal, Vol. I, 5.ª Edição, pp. 731 e ss.).

como referimos, os metadados são guardados em ficheiros informáticos encriptados e separados de todos os demais ficheiros e só poderão ser desencriptados e acedidos os metadados que disserem respeito ao arguido, ao suspeito, ao intermediário ou à vítima (e, neste caso, apenas mediante consentimento) – e não os metadados de todo e qualquer cidadão –, exclusivamente para a investigação, deteção e repressão de crimes graves por parte das autoridades competentes e mediante despacho fundamentado; e acresce que a utilização de metadados conservados pode inclusivamente ter lugar no interesse do respetivo titular, designadamente quando seja a vítima do crime ou quando, sendo arguido ou suspeito, os metadados possam demonstrar a sua inocência ou, no mínimo, gerar uma dúvida razoável quanto à sua culpabilidade[271].

O segundo problema prende-se com a inexequibilidade/inviabilidade da exigência de que a conservação de metadados seja limitada aos dados relativos a pessoas que possam estar envolvidas de alguma forma numa infração grave e/ou a pessoas cujos metadados, se conservados, possam contribuir, por outras razões (diversas do envolvimento numa infração grave), para a luta contra a criminalidade grave. E é inexequível/inviável, uma vez que a conservação de metadados a que se refere a Lei n.º 32/2008 é uma medida de prevenção criminal que se integra na chamada investigação proativa (que é essencial para responder às novas formas de criminalidade, em que uma investigação meramente reativa, *i.e.*, apenas a partir da obtenção da notícia do crime, é manifestamente ineficaz), sendo que a investigação proativa inicia-se num momento prévio à prática do crime ou ao conhecimento da sua prática pelas autoridades e visa, entre outras finalidades, obter uma *notitia criminis*, obter informações que facilitem a investigação de crimes que venham a ser cometidos[272] ou relativas ao modo de funcionamento de certas

[271] Porquanto, *de jure condito*, as proibições de prova, salvo no caso específico do art. 126.º, n.º 4, do CPP, tornam as provas nulas e inutilizáveis, independentemente de favorecerem a acusação ou a defesa (cfr. DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 1, p. 571).

[272] Como também sucede no caso dos deveres de colaboração/reporte ao abrigo da Lei n.º 83/2017, de 18 de agosto, em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo, e no caso da recolha de ADN de arguidos condenados, nos termos do art. 8.º, n.ºs 2 e 3, da Lei n.º 5/2008, de 12 de fevereiro.

formas de criminalidade[273] (as chamadas informações de *intelligence*) ou evitar o cometimento de crimes já planeados ou minimizar os seus efeitos para as vítimas[274].

Dito de outro modo, num momento prévio à obtenção da notícia do crime é *impossível* delimitar o âmbito dos metadados a conservar nos termos pretendidos pelo TC (e também pelo TJUE). No fundo, o TC (e o TJUE) formulou uma exigência que é de observância impossível e que contradiz a natureza preventiva, proativa da conservação de metadados e, com isso, declarou a inconstitucionalidade dos arts. 4.º e 6.º da Lei n.º 32/2008, negando, na prática – salvo se for possível encontrar vias alternativas no Direito vigente[275] – a possibilidade de utilização de metadados na investigação criminal, que é um meio absolutamente e cada vez mais necessário para responder às mais graves formas de criminalidade da atualidade.

E, por fim, o juízo de inconstitucionalidade formulado pelo TC no Acórdão do n.º 268/2022 é inconstitucional também por uma outra razão.

Com efeito, o decidido pelo TC, no caso de não ser possível encontrar vias alternativas aos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008 no Direito vigente para obter metadados para as investigações criminais (o que, como referimos, está longe de ser pacífico), pode ter (como já está a ter[276]) consequências devastadoras para a resposta à criminalidade (e, como tal, para a proteção dos direitos fundamentais dos cidadãos[277]), para o restabelecimento da paz jurídica e para a credibilidade da Justiça e do próprio Estado de Direito, uma vez que:

---

[273] Que também visam simplificar o combate a essas formas de criminalidade no futuro, como sucedeu, por exemplo, nos Estados Unidos e na Itália, em que as autoridades só lograram responder eficazmente à criminalidade organizada de tipo mafioso quando obtiveram informações (na maior parte dos casos, fornecidas por "arrependidos") acerca do chamado "método mafioso" (*i.e.*, o *modus operandi* da máfia).

[274] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 256-257.

[275] O que está longe de ser pacífico entre nós, como é demonstrado pelo levantamento de jurisprudência que realizámos supra.

[276] Veja-se, por exemplo, o sucedido quanto ao processo relativo ao assalto ao paiol de armas de Tancos, em que o Tribunal da Relação de Évora anulou o acórdão do Tribunal de 1.ª Instância por força da valoração de metadados que haviam sido conservados, obrigando à prolação de uma nova decisão que não considere as provas relativas aos metadados (cfr. Acórdão da RE de 28/02/2023).

[277] Pois a prática de crimes também constitui um atentado contra os direitos fundamentais dos cidadãos em geral e das vítimas em particular.

a) Nos processos em curso, não poderão ser obtidos metadados conservados e aqueles que tiverem sido obtidos não poderão ser usados como prova, o que pode comprometer de sobremaneira a eficácia das investigações e conduzir a decisões absolutórias[278] materialmente injustas, bem como, na medida em que também a defesa fica impossibilitada de os usar, conduzir a decisões condenatórias materialmente injustas; e

b) No caso de condenações transitadas em julgado (sobretudo no caso de crimes graves, de criminosos perigosos e/ou de condenações em penas de prisão efetiva), existe o risco[279] de, nos processos em que os metadados tenham sido decisivos para a condenação[280], indivíduos que comprovadamente cometeram crimes (e, por isso, foram condenados) acabarem por ser absolvidos, com tudo o que isso possa acarretar em termos de prevenção geral e especial, para as vítimas do crime (que poderão vir a ser confrontadas com a absolvição de criminosos que haviam efetivamente cometido crimes contra si e que haviam sido condenados com trânsito em julgado) e, em última análise, para a credibilidade da Justiça e do Estado de Direito aos olhos dos cidadãos; e, mesmo no caso do condenado, as provas que os metadados podem proporcionar também podem servir para, em sede de recurso de revisão, suscitar uma dúvida fundada quanto à justiça da sua condenação[281].

---

278 Nas "decisões absolutórias" devemos incluir, além das sentenças absolutórias, os despachos de arquivamento (no inquérito) e os despachos de não pronúncia (na instrução).

279 Embora as condenações transitadas em julgado só possam ser postas em causa por via da interposição de um recurso extraordinário de revisão e o STJ, como vimos, tenha negado, até ao momento, provimento a todos os recursos de revisão interpostos com este fundamento, esse risco não está totalmente afastado, pois as decisões do STJ são passíveis de recurso de constitucionalidade e a própria jurisprudência do STJ pode sofrer alteração.

280 Designadamente nas situações em que tenha sido através dos metadados que foi possível identificar os suspeitos ou um determinado círculo de suspeitos (e, desse modo, dirigir a investigação para esses indivíduos) e/ou obter as provas que sustentaram a condenação (sendo que dificilmente teria sido possível descobrir/obter sem a prévia obtenção dos metadados) ou em que, no caso de condenações com base em prova indiciária, tenham sido os metadados que permitiram retirar dos indícios a prova dos factos constitutivos do crime.

281 *V.g.*, os metadados relativos ao arguido A no processo X (e que não eram conhecidos no processo Z, pois o arguido A jamais fora arguido, suspeito, intermediário ou vítima) podem

Deste modo, o entendimento do TC no Acórdão n.º 268/2022 é também incompatível com o princípio da proporcionalidade (e, como tal, inconstitucional), que não possui apenas uma vertente de proibição do excesso (*Übermaßverbot*), possuindo igualmente uma vertente de proibição de insuficiência (*Untermaßverbot*), que é violada quando as entidades (designadamente, o Estado em todas as suas funções: legislativa, jurisdicional e administrativa) oneradas com um dever de proteção (*Schutzpflicht*) não adotam medidas ou adotam medidas insuficientes para garantir uma proteção constitucionalmente adequada dos direitos fundamentais[282], aí se incluindo, por exemplo, a adoção de medidas inadequadas ou ineficazes, o não aperfeiçoamento das medidas existentes, a adoção de medidas que desprotejam os cidadãos face às ameaças ou agressões provenientes de outros cidadãos e a "anulação" de medidas existentes de que resulte uma proteção insuficiente de direitos fundamentais[283]. E a proibição de insuficiência vale também no plano do Direito penal (e processual penal)[284], sendo que, como bem afirma ISENSEE[285], o cumprimento do dever estatal de proteção da segurança dos cidadãos tanto poderá consistir na adoção de medidas repressivas como de medidas preventivas.

---

levar ao surgimento de dúvidas fundadas quanto à justiça da condenação de B no processo Z.

[282] Assim, GOMES CANOTILHO, Direito Constitucional e Teoria da Constituição, p. 273, segundo o qual, ocorre um defeito de proteção (e, como tal, uma violação *Untermassverbot*) «*quando as entidades sobre quem recai um dever de proteção (Schutzpflicht) adoptam medidas insuficientes para garantir uma proteção constitucionalmente adequada dos direitos fundamentais*».

[283] Cfr. ISENSEE, Das Grundrecht auf Sicherheit, p. 40, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, p. 68, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 322, HAIN, "Der Gesetzgeber in der Klemme zwischen Übermass- und Untermassverbot", *in* DVBl, 1993, p. 983, UNRUH, Zur Dogmatik der grundrechtlichen Schutzpflichten, pp. 24-25, e PIETRZAK, "Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte", *in* JuS, 1994, pp. 750 e 752-753.

[284] Acerca dos corolários do princípio da proporcionalidade na vertente de proibição de insuficiência e dos deveres estatais de proteção ao nível do Direito penal (em sentido amplo), *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 330 e ss., com vastas referências doutrinárias e jurisprudenciais.

[285] ISENSEE, "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", *in* Handbuch des Staatsrechts der Bundesrepublik Deutschland, V, 2.ª Edição, p. 218.

É evidente que a proibição de insuficiência não pode ser radicalizada, sob pena de ultrapassagem dos limites de facto e direito a que o legislador está adstrito numa Sociedade livre e democrática[286], mas também não pode ser desvalorizada ao ponto de a esvaziar ou quase esvaziar de efeito útil em favor da proibição do excesso, jamais se podendo afirmar que a proibição de insuficiência apenas vale na medida do possível[287].

A proibição de insuficiência corresponde ao patamar mínimo de proteção do direito fundamental, ao passo que a proibição do excesso corresponde ao patamar máximo admissível da restrição, vigorando a liberdade de conformação do legislador (que define o "*como*" da proteção dos direitos fundamentais dos cidadãos face a ameaças ou a agressões provenientes de terceiros) no espaço que medeia entre o patamar mínimo de proteção e o limite máximo da restrição[288].

Na medida em que, no momento da aplicação ao caso concreto, ambas as vertentes do princípio da proporcionalidade poderão colidir entre si, haverá que compatibilizá-las, encontrando a proibição de insuficiência limites na proibição do excesso e vice-versa, pois a violação da proibição de insuficiência também pode resultar de uma incorreta aplicação da proibição do excesso e vice-versa[289].

Em suma, o entendimento perfilhado no Acórdão do TC n.º 268/2022 é ele próprio inconstitucional, porquanto dele resulta uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 ao impossibilitar a conservação e o acesso a esses dados nos termos dos arts. 4.º, 6.º e 9.º dessa Lei, quando:

---

[286] Cfr. VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 149, ISENSEE, "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", *in* Handbuch des Staatsrechts der Bundesrepublik Deutschland, V, 2.ª Edição, p. 155, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 325.

[287] Como faz VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 149 [sobre a nossa crítica a esta afirmação, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 330 (nota 1269)].

[288] Neste sentido, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 328.

[289] Assim, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 328-329.

a) a conservação de metadados, sobretudo tendo em conta o modo como os mesmos são armazenados nos termos da lei, não restringe qualquer direito fundamental;
b) ainda que o acesso aos metadados restringisse direitos fundamentais, fá-lo-ia sempre de uma forma pouco intensa (pelas razões sobreditas), jamais justificando a proteção desses direitos fundamentais (para mais quando são alvo de uma restrição pouco intensa) a completa desconsideração das necessidades de resposta eficaz aos crimes graves constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e de proteção dos direitos fundamentais protegidos por via da criminalização dessas condutas;
c) assenta em exigências impossíveis de cumprir em face da natureza preventiva da conservação de metadados e cujo (inevitável) incumprimento é utilizado como fundamento para declarar a inconstitucionalidade;
d) é manifestamente excessivo declarar a inconstitucionalidade de uma norma e, com isso, vedar o recurso a um meio de obtenção de prova absolutamente essencial para investigar crimes graves (e para o arguido demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável) com fundamento em essa norma não prever a obrigatoriedade da notificação dos titulares dos dados de que os seus dados foram acedidos pelas autoridades quando, pela sua natureza, não caberia a essa norma regular uma tal matéria e, na maioria das situações, essa notificação é desnecessária e redundante, dado que os dados acedidos são os dados dos arguidos, que, tendo acesso aos autos, têm conhecimento de que os seus dados foram acedidos e poderão exercer os seus direitos a esse respeito; e
e) irá dificultar de sobremaneira a resposta à criminalidade grave ao impedir – caso não seja possível encontrar no Direito vigente uma via alternativa, o que está longe de ser pacífico – a conservação preventiva dos metadados e a sua utilização probatória nos processos em curso e, no caso de condenações transitadas em julgado, poderá abrir a porta a insustentáveis

situações de impunidade com a absolvição de criminosos que haviam sido condenados por sentenças transitadas em julgado.

Ademais, como referimos, o entendimento do TC viola igualmente o princípio da não discriminação no tratamento de dados pessoais (arts. 35.º, n.º 3, da CRP, 14.º da CEDH e 21.º, n.º 1, da CDFUE), o princípio da presunção da inocência (arts. 32.º, n.º 2, 1.ª parte, da CRP, 6.º, §2.º, da CEDH e 48.º, n.º 1, da CDFUE), o disposto nos arts. 8.º, n.º 4, *in fine*, da CRP e 53.º da CDFUE e, no caso de o arguido/condenado ser impossibilitado de demonstrar a sua inocência ou de gerar uma dúvida razoável acerca da sua culpabilidade ou da justiça da sua condenação, o entendimento do TC viola igualmente o princípio do processo equitativo (cfr. arts. 32.º, n.º 1, da CRP, 6.º da CEDH e 47.º da CDFUE).

E reiteramos que a impossibilidade de conservação e de utilizabilidade probatória de metadados conservados poderá conduzir a condenações do Estado Português no TEDH e no pagamento de indemnizações às vítimas por responsabilidade civil no exercício da função jurisdicional.

7. As possibilidades de conservação e utilização de metadados em processos penais em curso após a declaração de inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho

Pese embora a declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, como acabámos de referir, torna-se imperativo[290] procurar caminhos alternativos no nosso Direito vigente.

Começando pelas normas não declaradas inconstitucionais que permitem obter metadados previamente conservados para o processo são, para quem, como

[290] A fim de obstar à violação do princípio da proibição de insuficiência por via do défice de proteção dos direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (pese embora consideremos que o art. 9.º da Lei n.º 32/2008 fora revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, aplicando-se aos dados de tráfego o catálogo do art. 18.º, n.º 1, desta Lei e inexistindo catálogo relativamente aos dados de localização e de base) e evitar condenações do Estado português no TEDH (por força dos deveres positivos de levar a cabo investigações criminais relativamente a crimes que lesem direitos fundamentais garantidos pela CEDH que o TEDH tem considerado recaírem sobre as autoridades) e condenações no pagamento de indemnizações às vítimas por responsabilidade civil no exercício da função jurisdicional.

nós, considera que o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009[291]:

a) no caso dos dados de base e de localização[292]: art. 14.º, n.º 4, da Lei n.º 109/2009; e

[291] Acerca desta questão, com maiores desenvolvimentos, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 564, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 64 e ss.

[292] RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 50 e ss., considera que o art. 14.º, n.º 4, da Lei n.º 109/2009 não permite a obtenção de dados de localização, na medida em que a al. c) desse n.º 4 (à semelhança do que sucede com o art. 18.º, n.º 3, al. c), da CCiber) exige que tais dados estejam disponíveis com base num contrato ou acordo de serviços; ora, a partir do momento que esses dados estão na posse do fornecedor de serviços em virtude do próprio contrato de prestação de serviços de comunicações eletrónicas, não vemos em que medida o art. 14.º, n.º 4, da Lei n.º 109/2009 não permite a obtenção de dados de localização que estejam na posse do fornecedor de serviços; ademais, o art. 14.º, n.º 4, da Lei n.º 109/2009 permite expressamente a obtenção de dados informáticos que não sejam dados de conteúdo nem dados de tráfego (e os dados de localização, tal como os dados de base, não são uma coisa nem outra).

b) no caso dos dados de tráfego: arts. 18.º, n.º 2, da Lei n.º 109/2009[293] (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais)[294].

Diversamente, para quem entenda que o art. 9.º da Lei n.º 32/2008[295] não foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009:

a) no caso dos dados de base: art. 14.º, n.º 4, da Lei n.º 109/2009; e

---

[293] Na medida em que sempre considerámos que o art. 9.º da Lei n.º 32/2008 revogou parcialmente o art. 189.º, n.º 2, do CPP e que, posteriormente, o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009 (apesar do disposto no seu art. 11.º, n.º 2) e tendo em conta que (1) as comunicações a que se refere o art. 18.º da Lei n.º 109/2009 também geram dados de tráfego e (2) a Lei n.º 109/2009 contém aquilo que podemos denominar como o regime geral da prova digital, o regime relativo à obtenção de dados de tráfego que houvessem sido conservados à luz da Lei n.º 32/2008 terá de constar da Lei n.º 109/2009, como efetivamente consta. De resto, se o art. 9.º da Lei n.º 32/2008 revogou parcialmente o art. 189.º, n.º 2, do CPP, revogado aquele preceito pelos arts. 12.º e ss. da Lei n.º 109/2009 não poderá repristinar-se o art. 189.º, n.º 2, do CPP, apenas restando buscar a norma habilitante da obtenção de dados de tráfego previamente conservados na Lei n.º 109/2009.

Para além disso, o art. 18.º da Lei n.º 109/2009 revogou parcialmente o art. 189.º, n.º 1, do CPP.

Deste modo, também a obtenção, em tempo real, de dados de tráfego gerados no âmbito das comunicações a que se refere o art. 18.º da Lei n.º 109/2009 terá de estar prevista na Lei n.º 109/2009 (pois o art. 187.º do CPP apenas inclui as comunicações por telefone e o art, 189.º, n.º 1, do mesmo Código apenas inclui as conversações entre presentes), como efetivamente consta.

E, por isso, a norma habilitante para a obtenção, em tempo real, de dados de tráfego gerados no âmbito das comunicações a que se refere o art. 18.º da Lei n.º 109/2009 é esse mesmo art. 18.º (pois o art. 14.º exclui os dados de tráfego), por via de uma interpretação hábil do n.º 2 do art. 18.º na parte em que se refere ao "registo de transmissões de dados informáticos". E, igualmente por via de uma interpretação hábil do art 18.º, n.º 2 (e também por igualdade de razão face à obtenção do mesmo tipo de dados em tempo real), a obtenção de dados de tráfego previamente conservados (que restringe direitos fundamentais da mesma forma e na mesma medida que a obtenção em tempo real) também é subsumível ao art. 18.º, n.º 2.

Sem embargo, a fim de afastar quaisquer dúvidas a este respeito, consideramos que a redação do art. 18.º, n.º 2, da Lei n.º 109/2009 deveria ser aperfeiçoada.

[294] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", *in* Comentário do Código de Processo Penal, Vol. I, 5.ª Edição, p. 860, e DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 2, p. 681, e também em "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 48-49.

[295] Que, por sua vez, havia revogado o art. 189.º, n.º 2, do CPP relativamente à obtenção, na fase de inquérito, de dados de tráfego e de localização previamente conservados para a investigação de crimes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 564-565, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, p. 58).

b) no caso dos dados de tráfego e de localização, art. 189.º, n.º 2, do CPP[296].

É certo que o TC – embora de uma forma completamente desproporcionada e desrazoável – considerou que o art. 9.º da Lei n.º 32/2008 é inconstitucional em virtude de não estar prevista a obrigatoriedade da notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros. Todavia, tal poderá ser colmatado por via de, apesar de a Lei não o prever, a autoridade judiciária notificar as pessoas cujos metadados tenham sido acedidos logo que essa notificação não seja suscetível de comprometer as investigações (quer a investigação naquele processo quer noutros processos) nem a vida, a integridade física ou a liberdade (incluindo a liberdade e a autodeterminação sexual) de terceiros[297].

Deste modo, as autoridades podem legitimamente aceder, para fins de investigação criminal, a metadados previamente conservados pelos operadores de comunicações eletrónicas[298].

---

[296] Cfr. RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 74-75, e Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

[297] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 49.

[298] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", *in* Comentário do Código de Processo Penal, Vol. I, 5.ª Edição, p. 860, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 48-49, RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 74-75, e Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

Mesmo antes da entrada em vigor da Lei n.º 109/2009, dado que antes desse momento (e da entrada em vigor da Lei n.º 32/2008) já vigoravam o art. 189.º, n.º 2 (ao abrigo do qual era possível obter dados de tráfego e de localização celular, não distinguindo a Lei se se tratava de dados obtidos em tempo real ou de dados conservados) e os arts. 125.º e 135.º (à luz dos quais era possível obter os dados de base), todos do CPP.

No entanto, para que esse acesso (e ulterior valoração) possa ter lugar, os metadados terão de ter sido conservados e, mais do que isso, terão de ter sido legitimamente conservados, pelo que, em face da declaração de inconstitucionalidade dos arts. 4.º e 6.º da Lei n.º 32/2008, terá(ão) de existir, na nossa ordem jurídica, outra(s) norma(s) que preveja(m) a possibilidade de conservar metadados.

E, de facto, nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho (normas que não foram declaradas inconstitucionais pelo TC), os prestadores de serviços de comunicações eletrónicas podem conservar metadados durante 6 meses (que é o período durante o qual a fatura pode ser legalmente contestada e em que o respetivo pagamento pode ser exigido) para fins de faturação dos serviços prestados.

Ainda que a finalidade dessa conservação não seja a utilização probatória dos dados conservados em processos penais, consideramos que, se essa conservação é legalmente admissível para efeitos de salvaguarda de direitos privados de cariz patrimonial dos prestadores de serviços de comunicações eletrónicas (cobrança dos serviços prestados), por maioria de razão, é igualmente legítimo o acesso das autoridades a tais dados (legitimamente conservados) para fins de investigação criminal, prosseguindo-se, dessa forma, o interesse público numa Justiça penal funcionalmente eficaz (que é um pressuposto essencial do Estado de Direito e possui, também ele, respaldo constitucional), sendo que a investigação dos crimes e a punição dos criminosos é levada a cabo em prol do interesse da Comunidade no seu todo e não em prol do engrandecimento do Estado nem de interesses meramente privados[299].

Ademais, antes da entrada em vigor da Lei n.º 32/2008 e da reforma de 2007 do CPP, a jurisprudência admitia a obtenção de dados de tráfego (que eram conservados à luz da Lei n.º 41/2004) junto dos operadores de comunicações eletrónicas (cfr., entre outros, Acórdãos da RC de 17/05/2006 e 15/11/2006, da RG de 10/01/2005 e 21/11/2005 e da RE de 26/06/2007).

[299] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", *in* Comentário do Código de Processo Penal, Vol. I, 5.ª Edição, p. 859, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 50, e RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, p. 72.

A isto acresce que, como referimos, os arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho, não foram declarados inconstitucionais pelo TC.

And last but not least, é este o entendimento que permite obstar a violações do princípio da proporcionalidade (na vertente de proibição de insuficiência) e evitar condenações do Estado português no TEDH e no pagamento de indemnizações às vítimas, por responsabilidade civil no exercício da função jurisdicional.

Deste modo, consideramos que os metadados conservados pelos prestadores de serviços de comunicações eletrónicas nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004 podem ser utilizados em processos penais[300], assim se obtendo uma concordância prática adequada entre os direitos fundamentais em colisão e obstando aos efeitos nefastos que a impossibilidade de acesso, obtenção e valoração de metadados para fins de investigação criminal poderá ter nos processos em curso (como tem tido) e, sobretudo, nas condenações transitadas em julgado que referimos supra.

E, como também referimos supra, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável.

No entanto, contra este nosso entendimento poderão ser aduzidos vários argumentos, que se nos afiguram totalmente improcedentes.

Assim, em primeiro lugar, poderá aduzir-se que o entendimento que defendemos constitui, na fase de utilização dos metadados, por uma "alienação do fim" ("Z*weckentfremdung*"), pois, ao serem subsequentemente acedidos e

[300] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", *in* Comentário do Código de Processo Penal, Vol. I, 5.ª Edição, p. 859, DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 2, p. 681, e também em "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, p. 50, RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 61 e ss., e Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023; contra, Acórdãos da RL de 25/10/2022, da RP de 07/09/2022, 07/12/2022 e 24/05/2023, da RC de 12/10/2022 e da RE de 25/10/2022, 28/02/2023, 09/05/2023 e 12/09/2023.

valorados num processo penal, os metadados irão ser utilizados para uma finalidade diversa daquela para a qual foram conservados[301]. E, de facto, é isso que acontece.

Contudo, pese embora o que parece resultar do Acórdão do TC n.º 268/2022 (e também do Acórdão Digital Rights), o direito à autodeterminação informacional (de que a proibição de "alienação do fim" é um instrumento de tutela) não é absoluto e, além disso, como referimos, a mera conservação de metadados não restringe quaisquer direitos fundamentais (sendo que é a própria Lei n.º 41/2004 que "informa" os utilizadores de comunicações eletrónicas de que os seus metadados podem ser conservados pelos fornecedores de tais serviços) e o ulterior acesso aos mesmos restringe direitos fundamentais de uma forma que não é qualificável como intensa. E, estando em causa a resposta à criminalidade grave, a "alienação do fim" jamais poderá constituir um óbice à obtenção e valoração de metadados para fins de investigação criminal, sob pena de violação da proibição de insuficiência e dos direitos fundamentais a que se reconduzam os bens jurídicos tutelados pelos crimes em causa no caso concreto e que sejam superiores aos direitos à intimidade/privacidade e à autodeterminação informacional[302].

Em segundo lugar, poderá aduzir-se que o TJUE entende que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE (que foi transposta para o Direito português por via da Lei n.º 41/2004), conforme alterada pela Diretiva 2009/136/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da CDFUE, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que preveja, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica, bem como a uma regulamentação nacional que regule a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades

[301] Argumento aduzido nos Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[302] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* RMP, n.º 170, pp. 50-51, e no essencial (dado que considera que não existe qualquer mudança de finalidade, que, na realidade existe, pois os metadados foram conservados para outra finalidade que não a utilização em processo penal), RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* RMP, n.º 172, pp. 65-66.

nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União Europeia.

No entanto, os dados conservados nos termos da Lei n.º 41/2004 não se destinam à investigação criminal (como sucedia no caso da Diretiva 2006/24/CE e da Lei n.º 32/2008), pelo que – sem prejuízo das críticas que formulámos supra – a jurisprudência do TJUE não impede a conservação de metadados para as finalidades previstas na Lei n.º 41/2004.

Em terceiro lugar, poderá argumentar-se que aplicar o regime dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009, seria "*deixar entrar pela janela*" aquilo a que o Acórdão do TC n.º 268/2022 "*fechou a porta*", pois o regime que resultaria da aplicação dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009 padece da mesma falta de garantias que levou à declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei nº 32/2008[303]. No entanto, tendo em conta a crítica que formulámos ao Acórdão do TC n.º 268/2022, "*deixar entrar pela janela*" aquilo que que o TC terá "*fechado a porta*" mais não será do que evitar violações da própria Constituição e da CEDH (e até da CDFUE), bem como condenações do Estado Português no TEDH e no pagamento de indemnizações às vítimas, por responsabilidade civil no exercício da função jurisdicional.

Esta mesma resposta vale para o argumento de que, "caindo" a Lei n.º 32/2008 e na impossibilidade de aplicação do CPP e da Lei n.º 41/2004, recorrer às normas da Lei n.º 109/2009 seria seguir um caminho espúrio, tendo em conta a declaração de inconstitucionalidade e os fundamentos que a determinaram, não sendo lícito recorrer a "atalhos" como a invocação do disposto no art. 189.º do CPP ou na Lei n.º 109/2009 (para mais quando o art. 11.º, n.º 2, desta Lei determina que o disposto nos arts. 12.º a 19.º dessa Lei não prejudica o regime da Lei n.º 32/2008)[304].

Em quarto lugar, poderia aduzir-se que a aplicação da Lei n.º 109/2009 defraudaria o espírito do legislador, pois o desaparecimento da norma especial (*in*

[303] Como se faz no Acórdão da RP de 07/12/2022.

[304] Argumento aduzido no Acórdão da RC de 12/10/2022.

casu, os arts. 3.º e 9.º da Lei n.º 32/2008) não legitima a aplicação da norma geral (*in casu*, as normas da Lei n.º 109/2009)[305]. Contudo, dado que *lex specialis derogat legi generali*, inexistindo ou deixando de existir *lex specialis* (sendo certo que, como resulta do art. 282.º, n.º 1, do CPP, a declaração de inconstitucionalidade com força obrigatória geral produz efeitos *ex tunc* e implica a repristinação das normas revogadas pela norma declarada inconstitucional[306]), haverá que aplicar a *lex generalis*, razão pela qual não existe qualquer fundamento jurídico para negar a aplicabilidade das normas da Lei n.º 109/2009 e do art. 189.º, n.º 2, do CPP[307].

Em quinto lugar, também poderá argumentar-se que os Tribunais não podem substituir-se ao legislador, suprindo omissões de onde resultam graves inconvenientes para a investigação criminal[308]. No entanto, se os demais argumentos são improcedentes, este argumento, mais do que ser também improcedente, é absolutamente inaceitável, pois assenta numa visão completamente ultrapassada dos direitos fundamentais, considerando-os apenas na sua vertente negativa (enquanto *Abwehrrechte*, ou seja, direitos de defesa dos particulares contra os poderes públicos) e ignorando que – à luz da conceção social dos direitos fundamentais, que substituiu a conceção liberal, que os considerava apenas enquanto *Abwehrrechte*) – os direitos fundamentais possuem igualmente uma vertente positiva, prestacional (enquanto *Leistungsrechte*), que obriga o Estado a proteger os direitos fundamentais dos cidadãos também contra ameaças/agressões provenientes de fontes não estatais (*v. g.*, de outros particulares) e da qual resultam os chamados deveres estatais de proteção (*Schutzpflichte*), cujo incumprimento configura a violação, pelo Estado, de direitos fundamentais e do princípio da

[305] Argumento esgrimido nos Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[306] Cfr. GOMES CANOTILHO, Direito Constitucional e Teoria da Constituição, pp. 1000-1001.

[307] Sendo que, para quem entenda que o art. 9.º da Lei n.º 32/2008 não foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, o art. 189.º, n.º 2, do CPP foi repristinado na parte relativa à obtenção de dados de tráfego e de localização previamente conservados, por via da declaração de inconstitucionalidade com força obrigatória geral do art. 9.º da Lei n.º 32/2008, como prevê o art. 282.º, n.º 1, da CRP.

Sobre o efeito repristinatório da declaração de inconstitucionalidade com força obrigatória geral relativamente às normas revogadas pela norma declarada inconstitucional, *vide* GOMES CANOTILHO, Direito Constitucional e Teoria da Constituição, pp. 1004-1005.

[308] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

proporcionalidade na vertente de proibição de insuficiência[309], que vale também no plano do Direito penal e processual penal[310]. E, como referimos supra, o incumprimento dos deveres estatais de proteção e a violação do princípio da proporcionalidade na vertente de proibição de insuficiência podem resultar, por exemplo, da adoção de medidas inadequadas ou ineficazes, do não aperfeiçoamento das medidas existentes, da adoção de medidas que desprotejam os cidadãos face às ameaças ou agressões provenientes de outros cidadãos ou da "anulação" de medidas existentes de que resulte uma proteção insuficiente de direitos fundamentais[311].

Ademais, os deveres estatais de proteção recaem sobre o conjunto das funções do Estado e não apenas sobre a função legislativa, pelo que também os Tribunais e a Administração estão vinculados ao cumprimento desses deveres, porquanto a proteção dos direitos fundamentais não se esgota na aprovação de leis, requerendo também a sua efetiva aplicação[312]; deste modo, o Estado, com a

---

309 Cfr., com maiores desenvolvimentos e amplas referências bibliográficas, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 331 e ss.

310 Acerca dos corolários do princípio da proporcionalidade na vertente de proibição de insuficiência e dos deveres estatais de proteção ao nível do Direito penal (em sentido amplo), *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 330 e ss., com vastas referências doutrinárias e jurisprudenciais.

311 Cfr. ISENSEE, Das Grundrecht auf Sicherheit, p. 40, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, p. 68, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 322, HAIN, "Der Gesetzgeber in der Klemme zwischen Übermass- und Untermassverbot", *in* DVBl, 1993, p. 983, UNRUH, Zur Dogmatik der grundrechtlichen Schutzpflichten, pp. 24-25, e PIETRZAK, "Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte", *in* JuS, 1994, pp. 750 e 752-753.

312 Cfr. ISENSEE, Das Grundrecht auf Sicherheit, p. 21, e também em "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", *in* Handbuch des Staatsrechts der Bundesrepublik Deutschland, V, 2.ª Edição, pp. 146, 147, 190-191 e 218-219, CANARIS, Direitos Fundamentais e Direito Privado, p. 124, GOMES CANOTILHO, "Omissões Normativas e Deveres de Proteção", *in* Estudos em Homenagem a Cunha Rodrigues, II, p. 119, JORGE REIS NOVAIS, As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, p. 88, VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 148, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 317-318 (incluindo a nota 1205), ROBBERS, Sicherheit als Menschenrecht, p. 125, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, pp. 63 e ss. e 180, e Sentença do BVerfG de 14/05/1985.

mediação do legislador ordinário ou, em caso de omissão deste, através da atuação dos Tribunais e da Administração, está obrigado a tomar medidas (normativas, judiciais e/ou fácticas) destinadas a proteger os direitos fundamentais contra ameaças/agressões de fontes diversas dos poderes públicos[313].

Este argumento desconsidera, igualmente, a circunstância de, como referimos, a investigação dos crimes e a punição dos criminosos constituírem um meio de proteção de direitos fundamentais e de, por isso, a eficácia da perseguição e da punição de criminosos (que dependem da eficácia da investigação enquanto instrumento de descoberta da verdade material e da obtenção das provas que a sustentam) ser imposta (e não meramente tolerada) pela Constituição e constituir, inclusivamente, um pressuposto essencial do Estado de Direito.

Daí que, para mais tendo em conta os efeitos nefastos da decisão do TC e que temos vindo a recensear ao longo deste estudo, os Tribunais não possam demitir-se de procurar caminhos alternativos aos arts, 4.º, 6.º e 9.º da Lei n.º 32/2008 com o argumento (inaceitável) de que compete ao legislador – e não aos Tribunais – solucionar o problema e suprir as omissões de que resultam graves inconvenientes para a investigação criminal, pois, com isso, os Tribunais estarão a demitir-se do seu dever constitucional e legal de proteger os direitos fundamentais dos cidadãos.

Em sexto lugar, também se argumenta[314] que não existe qualquer identidade formal ou material entre o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e o catálogo de crimes dos arts. 187.º, n.º 1, e 189.º do CPP e que, por isso, não há que aplicar, por repristinação, nenhuma norma do CPP (o que, de resto, implicaria o desrespeito pela opção do legislador de ter criado um catálogo mais restrito no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 em vez de considerar como "crimes graves" os

[313] Cfr. JORGE REIS NOVAIS, As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, p. 88, VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 148, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 317-318 (incluindo a nota 1205), ROBBERS, Sicherheit als Menschenrecht, p. 125, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, p. 64, Sentença do BVerfG de 16/10/1977, e, em casos-limite, ISENSEE, "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", *in* Handbuch des Staatsrechts der Bundesrepublik Deutschland, V, 2.ª Edição, pp. 230-231 (alterando a sua opinião anterior); contra, ISENSEE, Das Grundrecht auf Sicherheit, p. 43, UNRUH, Zur Dogmatik der grundrechtlichen Schutzpflichten, p. 24, e DIETLEIN, Die Lehre von den grundrechtlichen Schutzpflichten, 2.ª Edição, p. 72.

[314] Cfr. Acórdão da RC de 12/10/2022.

crimes constantes do catálogo do n.º 1 do art. 187.º do CPP). Todavia, além de entendermos que o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009 (apesar da redação do art. 11.º, n.º 2, desta Lei)[315], a opção do legislador ao criar um catálogo mais restrito no caso do acesso aos metadados conservados do que no caso da obtenção de metadados em tempo real não faz qualquer sentido[316], pelo que não vemos qualquer inconveniente em aplicar a Lei n.º 109/2009 neste tipo de situações. E, quanto à pretensa não repristinação das normas do CPP na sequência da declaração de inconstitucionalidade do art. 9.º da Lei n.º 32/2008, vale o que referimos supra quanto ao argumento de que o desaparecimento da norma especial (*in casu*, os arts. 3.º e 9.º da Lei n.º 32/2008) não legitima a aplicação da norma geral (*in casu*, as normas da Lei n.º 109/2009), incluindo no que tange à incompatibilidade deste argumento com o art. 282.º, n.º 1, da CRP.

Em sétimo lugar, aduz-se[317], igualmente, que, tendo em conta os fundamentos da declaração de invalidade da Diretiva 2006/24/CE pelo TJUE, o regime da Lei n.º 32/2008 teria de ser ainda mais restritivo (e daí a declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º desta Lei), sendo certo que o regime do art. 189.º, n.º 2, do CPP é menos exigente do que o regime da Lei n.º 32/2008 e que obter ou valorar metadados conservados com base no art. 189.º, n.º 2, do CPP, na Lei n.º 41/2004 e na Lei n.º 109/2009 equivaleria a que a declaração de inconstitucionalidade produzisse o efeito contrário àquele que pretendeu (pois permitiria a aplicação de um regime menos restritivo do que o regime dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008).

Relativamente a estes argumentos, tendo em conta tudo o que temos vindo a referir (incluindo o que referimos quanto à jurisprudência do TJUE em matéria de metadados e ao Acórdão do TC n.º 268/2022), o facto de o regime que resulta da aplicação do art. 189.º, n.º 2, do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009 ser – e

---

315 Relativamente às razões que, na nossa ótica, conduzem a uma tal conclusão, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 563-563, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 65 e ss., com maiores desenvolvimentos e referências bibliográficas.

316 Pois a obtenção e a valoração de metadados conservados não restringem direitos fundamentais de uma forma mais intensa do que a obtenção desses metadados em tempo real e subsequente valoração.

317 Cfr. Acórdão da RC de 12/10/2022.

é, e bem – menos restritivo do que o regime do art. 9.º da Lei n.º 32/2008 não é minimamente impeditivo da obtenção e valoração probatória, em processos penais, de metadados conservados pelos prestadores de serviços de comunicações eletrónicas nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004.

Por isso, reiteramos que, apesar do decidido pelo TC no seu Acórdão n.º 268/2022, são lícitas, à luz da legislação vigente, a obtenção e valoração probatória, em processos penais, de metadados conservados pelos prestadores de serviços de comunicações eletrónicas nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, assim como, na nossa ótica, o entendimento contrário, além de não ter apoio na Lei, viola a CRP, a CEDH e mesmo a própria CEDFUE.

8. As alterações à Lei n.º 32/2008 aprovadas pela Assembleia da República. A nossa apreciação

Ciente da absoluta necessidade da conservação e da utilização probatória de metadados conservados na investigação criminal, o legislador, apesar da estreitíssima (ou mesmo inexistente) margem de manobra que lhe foi deixada pelo Acórdão do TC n.º 268/2022 e pela própria jurisprudência do TJUE[318] posterior ao Acórdão Digital Rights, procurou elaborar nova legislação – introduzindo modificações na Lei n.º 32/2008 – relativa à conservação e à utilização probatória de metadados conservados na investigação criminal.

Tendo sido apresentados uma Proposta de Lei pelo Governo e Projetos de Lei pelo PSD, CH e PCP relativos à alteração da Lei n.º 32/2008 após o Acórdão do TC n.º 268/2002 e sido constituído um Grupo de Trabalho na Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República (no âmbito do qual fomos ouvidos, por indicação da IL), foi aprovado, em 13 de outubro de 2023, o Texto de substituição e relatório de nova apreciação na generalidade da Proposta de Lei n.º 11/XV/1.ª (GOV), e Projetos de Lei n.ºs 70/XV/1.ª (PSD), 79/XV/1.ª (CH) e 100/XV/1.ª (PCP). Tendo o diploma aprovado sido enviado para

[318] Que, atenta a situação de Portugal, no que tange à luta contra a criminalidade grave, apenas permitem a conservação generalizada e indiferenciada de endereços IP atribuídos à fonte de uma ligação e de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, uma vez que a conservação seletiva dos dados de tráfego e dos dados de localização nos termos propostos pelo TJUE é absolutamente inviável, como demonstrámos supra.

promulgação, o Presidente da República remeteu-o ao TC para fiscalização preventiva da sua constitucionalidade, o que se justifica plenamente.

O diploma aprovado, que reproduz a redação da Proposta de Lei n.º 11/XV/1.ª (GOV) e do Projeto de Lei n.º 70/XV/1.ª (PSD)[319], é, na nossa opinião, merecedor de elogio, mas também de algumas observações e críticas, salientando-se, desde já, a coragem do legislador ao insistir – pese embora a estreitíssima (ou mesmo inexistente) margem de manobra que lhe foi deixada pelo Acórdão do TC n.º 268/2022 e pela própria jurisprudência do TJUE posterior ao Acórdão Digital Rights – na previsão da conservação "preventiva" de metadados (incluindo no caso dos dados de tráfego e de localização) para efeitos de investigação criminal.

Vejamos, com maior pormenor, os aspetos mais relevantes das alterações introduzida pelo diploma aprovado à Lei n.º 32/2008.

8.1. Artigo 4.º da Lei n.º 32/2008

Concordamos com a exigência de que a conservação dos dados tenha lugar em Portugal ou no território de outro Estado-Membro da União Europeia, pois, desse modo, são cumpridas, sem qualquer margem para dúvidas, as exigências do TC e do TJUE e sem que daí resulte qualquer prejuízo para a investigação da criminalidade (*maxime* da criminalidade grave).

Ao ser mantido, quanto ao mais, o disposto no art. 4.º da Lei n.º 32/2008 entretanto julgado inconstitucional (seja a conservação "preventiva" sejam as tipologias de metadados a conservar) – aplaudindo-se a coragem do legislador neste ponto e a sua consciência quanto à absoluta necessidade deste instrumento para responder eficazmente à criminalidade –, não está a ser observada nem a jurisprudência do TC nem a jurisprudência do TJUE, visto que se trata de uma conservação generalizada e indiferenciada.

Todavia, tendo em conta o que viemos referindo quanto ao Acórdão do TC n.º 268/2022 e à jurisprudência do TJUE em matéria de conservação e utilização

---

[319] Disponível em https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c63793959566b786c5a793944543030764d554e425130524d5279394562324e3162575675644739 7a5357357059326c6864476c3259554e7662576c7a633246764c325a685a5442694d5749794c546b354f4755744e4468694e4330344d7a59304c5442685a4451344d57466c596a4d325a5335775a47593d&fich=fae0b1b2-998e-48b4-8364-0ad481aeb36e.pdf&Inline=true.

probatória de metadados, o legislador português só observará o disposto na CRP, na CEDH e mesmo na CDFUE se previr a conservação "preventiva" de metadados nos termos que já previa e volta a prever no art. 4.º da Lei n.º 32/2008, esperando-se que o TC repondere o entendimento desrazoável e inconstitucional que perfilhou no Acórdão n.º 268/2022.

Aliás, se dúvidas ainda existirem acerca da desrazoabilidade do entendimento do TJUE, que o TC acolheu, basta ver que, por exemplo, o legislador alemão, malgrado as várias tentativas que já levou a cabo nesse sentido, não consegue elaborar uma lei em matéria de conservação de metadados que o TJUE considere que observa o seu entendimento.

E a isto acresce que, se, por hipótese, na sequência do conflito entre o Estado de Israel e a organização terrorista Hamas, organizações terroristas islâmicas decidissem "acordar" os seus membros "adormecidos" que se encontrem em Estados-Membros da União Europeia, a continuar a vingar a jurisprudência do TJUE acolhida pelo TC e por um setor da jurisprudência dos Tribunais comuns, na maioria desses países, as autoridades não poderiam obter nem valorar dados de tráfego ou dados de localização que tivessem sido alvo de conservação e, após a ocorrência dos atentados, os dados de tráfego e/ou de localização obtidos em tempo real dificilmente teriam alguma utilidade para a investigação desses atentados.

Deste modo, ainda que existam caminhos alternativos no Direito vigente em matéria de conservação dos metadados e da sua utilização probatória em processos penais, é preferível voltar a prever expressamente essa possibilidade num diploma relativo ao combate à criminalidade, pois permite evitar quaisquer dúvidas, sobretudo quando continuam a ser proferidas decisões pelos Tribunais comuns que não autorizam a obtenção e utilização de metadados em processos penais e anulam as provas obtidas por via dos metadados conservados, rejeitando os caminhos alternativos que existem na Lei vigente.

8.2. Artigo 6.º da Lei n.º 32/2008

Relativamente ao n.º 1 do art. 6.º da Lei n.º 32/2008, na medida em que se entende maioritariamente que o IP é um dado de base[320], talvez se justificasse inverter a

[320] Sobre a subsunção do IP (estático e dinâmico) à categoria dos dados de base ou à categoria dos dados de tráfego, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 227 (nota 861), e também em Os meios de obtenção

ordem das als. b) e c), passando a constar da al. b) os "endereços de protocolo IP atribuídos à fonte de uma ligação" e da al. c) os "demais dados de base".

Passando ao n.º 2 do art. 6.º, existe uma incongruência face aos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho, pois, se os operadores de comunicações eletrónicas podem conservar os metadados por 6 meses para cobrança dos serviços prestados, por maioria de razão, no caso da conservação para fins de resposta à criminalidade grave, o prazo de conservação deveria ser, pelo menos, o mesmo[321].

Também não faz sentido presumir o consentimento no sentido da prorrogação do prazo de conservação para 6 meses até porque, no nosso Direito, no consentimento presumido, estão em causa situações de perigo na demora e de impossibilidade de obter o consentimento expresso em tempo útil, sendo que, no caso da conservação de metadados, não se verifica qualquer situação dessa natureza[322]. Além disso, para que o consentimento possa ser presumido, é necessário que seja razoável supor que, em face das circunstâncias do caso concreto, o visado teria prestado consentimento se tivesse sido consultado, não nos parecendo que seja possível formular uma tal suposição no que concerne à extensão do prazo de conservação de dados de tráfego e de dados de localização, sobretudo quando esses dados podem ser utilizados como prova contra o respetivo titular.

Quanto aos n.ºs 3 e 6, não nos parece que exista qualquer justificação para a atribuição da competência a um coletivo de Juízes do STJ: se um Tribunal de Comarca pode condenar em penas de 25 anos de prisão e um Juiz de 1.ª Instância pode determinar a prisão preventiva ou autorizar o recurso a meios de obtenção de prova muito mais restritivos de direitos do que a conservação de metadados (que nem sequer restringe direitos fundamentais), inexiste qualquer razão para que tenha de intervir um coletivo de Juízes do STJ.

De todo o modo, parecendo que a prorrogação prevista no n.º 3 dependerá da ocorrência de circunstâncias excecionais (como parece resultar do n.º 4), ao

---

de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 110-111, com referências doutrinais e jurisprudenciais.

321 Sem prejuízo de entendermos que o prazo de 1 ano, também no caso dos dados de tráfego e de localização, era razoável e não violava a Constituição.

322 Sobre o consentimento presumido, *vide* DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, pp. 460 e ss.

ponto de justificarem a intervenção do PGR, nesse caso, fará sentido que a prorrogação seja decidida pelo STJ, embora nos pareça excessiva a intervenção de um coletivo, sobretudo quando a mera conservação não restringe quaisquer direitos fundamentais.

Por fim, quanto ao n.º 5 do art. 6.º, existe o risco de este preceito vir a ser interpretado no sentido de constituir mais um argumento contra a admissibilidade da utilização probatória dos metadados armazenados nos termos da Lei n.º 41/2004, caso o TC, ao não reponderar o seu entendimento, volte a considerar que o art. 4.º e o art. 9.º da Lei n.º 32/2008 são inconstitucionais[323].

8.3. Artigo 7.º da Lei n.º 32/2008

As alterações introduzidas parecem-nos adequadas, existindo uma salutar preocupação em incrementar as garantias de inviolabilidade dos dados conservados.

8.4. Artigo 9.º da Lei n.º 32/2008

Pese embora sempre tenhamos entendido que, apesar do disposto no art. 11.º, n.º 2, da Lei n.º 109/2009, o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, entendemos que teria sido preferível introduzir melhoramentos na Lei n.º 109/2009 (por exemplo, introduzir o que consta dos n.ºs 7 a 9 do art. 9.º da Lei n.º 32/2008 nos arts. 14.º e 18.º da Lei n.º 109/2009, revogar o n.º 2 do art. 11.º da Lei n.º 109/2009, e clarificar a subsunção da obtenção dos dados de tráfego ao art. 18.º, n.º 2) em vez de reformular o art. 9.º da Lei n.º 32/2008.

De todo o modo, tendo o legislador optado por reformular o art. 9.º da Lei n.º 32/2008, nos termos em que o fez, concordamos com o aditamento daquilo que consta dos n.ºs 7 a 9 (a fim de observar a jurisprudência do TJUE e do TC); contudo, também entendemos que deveria ter sido estabelecida uma exceção relativa aos casos em que a notificação dos titulares dos metadados que tenham sido acedidos

[323] Por isso, apesar de termos inicialmente entendido que tal clarificação da lei se justificaria (como consta do documento que elaborámos para apoio à nossa audição Grupo de Trabalho dos Metadados da 1.ª Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República e que cedemos a esse Grupo de Trabalho), temos agora sérias reservas acerca da bondade do disposto no n.º 5 do art. 6.º da Lei n.º 32/2008.

possa prejudicar outras investigações em curso e não apenas a investigação em que os metadados foram utilizados.

No que tange ao n.º 2 do art. 9.º da Lei n.º 32/2008, tendo em conta o critério previsto nos arts. 268.º, n.º 2, e 269.º, n.º 2, do CPP[324], deveria prever-se, também aqui, a possibilidade de, em casos de perigo na demora, o pedido de acesso ser apresentado ao Juiz diretamente pela autoridade de polícia criminal ou mesmo a possibilidade de a autorização ser concedida pelo MP, embora com sujeição a ulterior ratificação *expressa* do Juiz (o que, na nossa ótica, não contradiz a jurisprudência do TJUE, pois existe uma intervenção, ainda que *a posteriori*, do Juiz).

O que consta dos demais números do art. 9.º da Lei n.º 32/2008 merece a nossa concordância, sem prejuízo de entendermos que o catálogo de crimes constante do art. 2.º, n.º 1, al. g), dessa Lei é excessivamente restritivo e que não se justifica a existência, na nossa ordem jurídica, de dois regimes diversos de obtenção de dados de localização e de dados de base, consoante a mesma ocorra em tempo real (a que se aplicará o regime do art. 14.º da Lei n.º 109/2009, que não contém qualquer elenco de crimes ou de alvos nem exige autorização judicial prévia na fase de inquérito) ou incida sobre dados conservados (a que se aplicaria o art. 9.º da Lei n.º 32/2008), porquanto o facto de os dados terem sido conservados não aumenta a lesividade da sua transmissão; e o mesmo vale quanto aos dados de tráfego, em que, se a obtenção ocorrer em tempo real, aplicar-se-á, consoante o entendimento, o art. 18.º da Lei n.º 109/2009 ou o art. 189.º, n.º 2, do CPP (cujos catálogos de crimes são muito mais amplos do que o do art. 2.º, n.º 1, al. g), da Lei n.º 109/2009), ao passo que, se incidir sobre dados conservados, aplicar-se-á o art. 9.º da Lei n.º 32/2008.

8.5. Artigos 16.º e 17.º da Lei n.º 32/2008

As alterações introduzidas afiguram-se-nos adequadas ao poderem proporcionar a deteção de situações menos corretas e a sua correção, quer para incrementar a eficácia da conservação e da utilização probatória de metadados quer para

[324] Em que se prevê a possibilidade de a autoridade de polícia criminal, em caso de urgência ou de perigo na demora, poder requerer diretamente ao JIC a prática de atos que devem ser praticados pelo JIC ou a autorização para a prática de atos que têm de ser autorizados pelo JIC.

impedir restrições desnecessárias e/ou desproporcionadas dos direitos fundamentais dos titulares dos metadados.

Conclusões

a) A Lei n.º 32/2008, de 17 de junho transpôs para a nossa ordem jurídica a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (metadados);
b) A conservação e a transmissão dos metadados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes, sendo obrigatória a separação dos ficheiros destinados à conservação de dados de quaisquer outros ficheiros para outros fins.
c) As provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável
d) Nos termos do art. 9.º da Lei n.º 32/2008, os metadados só podiam ser desbloqueados (*i.e.*, desencriptados) para efeitos de transmissão às autoridades competentes, que, nos termos do art. 2.º, n.º 1, al. f), são as autoridades judiciárias (Juiz, JIC e MP) e as autoridades de polícia criminal e, desde que se tratasse de metadados relativos ao arguido, ao suspeito, ao intermediário ou à vítima (neste último caso, mediante o respetivo consentimento);
e) O art. 9.º da Lei n.º 32/2008 fora já tacitamente revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, de 15 de setembro;
f) Na sequência de o TJUE, em 2014, ter declarado a Diretiva 2006/24/CE inválida e apesar das garantias previstas na Lei n.º 32/2008 (que não padecia dos vícios que haviam levado o TJUE a declarar a invalidade da Diretiva), o TC, embora com um voto de vencido, declarou a inconstitucionalidade, com força obrigatória geral, dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008;
g) O TJUE (no Acórdão Digital Rights) e o TC não realizaram qualquer ponderação entre os interesses em conflito, tendo desconsiderado, em

absoluto, os direitos fundamentais (garantidos pela CDFUE e pela CRP) prosseguidos através da investigação criminal;

h) Na sua jurisprudência relativa à conservação e à utilização probatória de metadados subsequente ao Acórdão Digital Rights, o TJUE passou a fundamentar as decisões com base numa ponderação de interesses, embora formulando exigências (1) impossíveis de cumprir, (2) desconformes com a realidade da criminalidade da atualidade, (3) de difícil (ou mesmo impossível) determinação e (4) que abrem a porta a um tratamento discriminatório entre os cidadãos;

i) A jurisprudência do TJUE relativa à conservação e utilização probatória de metadados viola a CEDH, a CRP e a própria CEDFUE;

j) O TC não estava obrigado a seguir a jurisprudência do TJUE no Acórdão Digital Rights (e, ao acolhê-la violou o disposto nos arts. 8.º, n.º 4, *in fine*, da CRP e 53.º da CDFUE), sendo que o Acórdão n.º 268/2022 padece de problemas ainda mais graves do que o Acórdão Digital Rights;

k) O entendimento plasmado no Acórdão do TC n.º 268/2022 (1) é desconforme com a realidade da criminalidade atual e da investigação dessa mesma criminalidade (cujas necessidades ignora em absoluto), (2) considera que mera conservação de metadados restringe direitos fundamentais, quando, na realidade, não restringe qualquer direito fundamental, (3) considera que a conservação generalizada e indiferenciada e a obtenção de dados de tráfego e de localização restringem direitos fundamentais de forma intensa, quando, na realidade, a obtenção de tais dados, ainda que restrinja direitos fundamentais, não o faz de uma forma intensa, (4) desconsidera, em absoluto, os direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, (5) considera inconstitucional a conservação de metadados para fins de investigação criminal de crimes graves, apesar de os prestadores de serviços de comunicações eletrónicas poderem conservar metadados durante 6 meses para fins de faturação dos serviços prestados, (6) é passível de comprometer seriamente a investigação de muitos crimes, (7) viola a CEDH, podendo conduzir a condenações do Estado Português no

TEDH e, na sequência dessas condenações, à condenação no pagamento de indemnizações às vítimas por responsabilidade civil no exercício da função jurisdicional, (8) viola o disposto nos arts. 8.º, n.º 4, *in fine*, da CRP e 53.º da CDFUE, (9) viola o princípio da presunção de inocência, (10) viola o princípio da não discriminação no tratamento de dados pessoais, (11) viola o princípio do processo equitativo, (12) viola o princípio da proporcionalidade na vertente de proibição de insuficiência e (13) pode conduzir a condenações e a absolvições materialmente injustas (em virtude da impossibilidade de obtenção e de valoração de metadados) e à revogação de condenações transitadas em julgado;

l) A Lei vigente permite evitar as consequências nefastas referidas na conclusão anterior, dado que o art. 14.º, n.º 4, da Lei n.º 109/2009 (no caso dos dados de base e de localização) e, no caso dos dados de tráfego, os arts. 18.º, n.º 2, da Lei n.º 109/2009 (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais) permitem obter dados de base, bem como os dados de tráfego e/ou de localização que tenham sido conservados pelos operadores de comunicações eletrónicas ao abrigo dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, ainda que essa conservação se destinasse à cobrança dos serviços prestados aos clientes;

m) O legislador aprovou já um diploma que introduz diversas alterações à Lei n.º 32/2008, em que tenta reformular o regime da conservação e da utilização probatória, em processos penais, de metadados conservados após a declaração de inconstitucionalidade, com força obrigatória geral, os arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, sendo essas alterações merecedoras da nossa concordância em alguns aspetos e da nossa crítica noutros.

Bibliografia

Andrade, José Carlos Vieira de – Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, Almedina, Coimbra, 2004.

Canaris, Claus-Wilhelm – Direitos Fundamentais e Direito Privado (traduzido por Ingo Wolfgang Sarlet e Paulo Mota Pinto), 2.ª Reimpressão, Almedina, Coimbra, 2009.

Canotilho, José Joaquim Gomes – "Omissões Normativas e Deveres de Protecção", *in* Estudos em Homenagem a Cunha Rodrigues, Volume II, pp. 111 e ss, Coimbra Editora, Coimbra, 2001.

Canotilho, José Joaquim Gomes – Direito Constitucional e Teoria da Constituição, 5.ª Edição, Almedina, Coimbra, 2002.

Canotilho, José Joaquim Gomes/Moreira, Vital – Constituição da República Portuguesa Anotada, Volume I, 4.ª Edição, Coimbra Editora, Coimbra, 2007.

Cardoso, Rui – "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", *in* Revista do Ministério Público, n.º 172, pp. 9 e ss., Lisboa, 2022.

Correia, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 29 e ss., Lisboa, 2014.

Dias, Jorge de Figueiredo – Acordos Sobre a Sentença em Processo Penal, O "Fim" do Estado de Direito ou um Novo "Princípio"?, Conselho Distrital do Porto da Ordem dos Advogados, Porto, 2011.

Dias, Jorge de Figueiredo – Direito Penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime, 3.ª Edição, Coimbra Editora, Coimbra, 2019.

Dietlein, Johannes – Die Lehre von den grundrechtlichen Schutzpflichten, 2.ª Edição, Duncker&Humblot, Berlim, 2005.

Hain, Karl-Eberhard – "Der Gesetzgeber in der Klemme zwischen Übermass- und Untermassverbot", *in* Deutsches Verwaltungsblatt, Ano 108, Fascículo 18, pp. 982 e ss., Carl Heymanns Verlag, Colónia, Berlim, Bona, Munique, 1993.

Isensee, Josef – Das Grundrecht auf Sicherheit, Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Walter de Gruyter, Berlim e Nova Iorque, 1983.

Isensee, Josef – "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", *in* Handbuch des Staatsrechts der Bundesrepublik Deutschland, Volume V, Allgemeine Grundrechtslehren, 2.ª Edição, pp. 143 e ss., C.F.Müller Juristischer Verlag, Heidelberg, 2000.

Júnior, José Paulo Baltazar – Crime Organizado e Proibição de Insuficiência, Livraria do Advogado, Porto Alegre, 2010.

Novais, Jorge Reis – As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, Coimbra Editora, Coimbra, 2003.

Nunes, Duarte Rodrigues – O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, Gestlegal, Coimbra, 2019.

Nunes, Duarte Rodrigues – "Da admissibilidade da obtenção de dados de localização celular ou de dados de tráfego de todos os telemóveis/cartões que acionaram um determinado conjunto de antenas/células de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado, para posterior identificação dos seus autores.", *in* Revista do Ministério Público, n.º 157, pp. 125 e ss., Lisboa, 2019.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, Gestlegal, Coimbra, 2021.

Nunes, Duarte Rodrigues – "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", *in* Revista do Ministério Público n.º 170, pp. 9 e ss., Sindicato dos Magistrados do Ministério Público, Lisboa, 2022.

Nunes, Duarte Rodrigues – Curso de Direito Penal, Parte Geral, Tomo I, Questões fundamentais, Teoria geral do crime, 2.ª Edição, Gestlegal, Coimbra, 2023.

Nunes, Duarte Rodrigues – Curso de Direito Processual Penal, 1, Noções gerais, Elementos do processo penal, Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues – Curso de Direito Processual Penal, 2, Elementos do processo penal (continuação), O procedimento criminal, Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues/Albuquerque, Paulo Pinto de – "Artigo 172.º", *in* Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Vol. I, 5.ª Edição, pp. 721 e ss., Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues/Albuquerque, Paulo Pinto de – "NOTA PRÉVIA ao Artigo 189.º", *in* Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Vol. I, 5.ª Edição, pp. 856 e ss., Universidade Católica Editora, Lisboa, 2023.

Pietrzak, Alexandra – "Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte", *in* Juristische Schulung, 1994, pp. 748 e ss., Verlag C. H. Beck, Munique e Frankfurt, 1994.

Robbers, Gerhard – Sicherheit als Menschenrecht, Aspekte der Geschichte, Begründung unsd Wirkung einer Grundrechtsfunktion, Nomos Verlag, Baden-Baden, 1987.

Unruh, Peter – Zur Dogmatik der grundrechtlichen Schutzpflichten, Duncker&Humblot, Berlim, 1996.

Jurisprudência

Tribunal Europeu dos Direitos Humanos

Acórdão McCann e Outros c. Reino Unido (de 27 de setembro de 1995), *in https://hudoc.echr.coe.int/*.

Acórdão Mahmut Kaya c. Turquia (de 28 de março de 2000), *in https://hudoc.echr.coe.int/*.

Acórdão Hugh Jordan c. Reino Unido (de 4 de maio de 2001), *in https://hudoc.echr.coe.int/*.

Acórdão Paul e Audrey Edwards c. Reino Unido (de 14 de março de 2002), *in https://hudoc.echr.coe.int/*.

Acórdão Nachova e Outros c. Bulgária (de 6 de julho de 2005), *in https://hudoc.echr.coe.int/*.

Acórdão Kaya e Outros c. Turquia (de 24 de outubro de 2006), *in https://hudoc.echr.coe.int/*.

Acórdão Ramsahai e Outros c. Países Baixos (de 15 de maio de 2007), *in https://hudoc.echr.coe.int/*.

Acórdão Angelova e Iliev c. Bulgária (de 26 de julho de 2007), *in https://hudoc.echr.coe.int/*.

Acórdão K.U. c. Finlândia (de 2 de dezembro de 2008), *in https://hudoc.echr.coe.int/*.

Acórdão Opuz c. Turquia (de 9 de junho de 2009), *in https://hudoc.echr.coe.int/*.

Acórdão Kolevi c. Bulgária (de 5 de novembro de 2009), *in https://hudoc.echr.coe.int/*.

Acórdão Al-Skeini e Outros c. Reino Unido (de 7 de julho de 2011), *in https://hudoc.echr.coe.int/*.

Acórdão Vasîlka c. Moldávia (de 11 de fevereiro de 2014), *in https://hudoc.echr.coe.int/*.

Acórdão Jaloud c. Países Baixos (de 20 de novembro de 2014), *in https://hudoc.echr.coe.int/*.

Acórdão Mustafa Tunç e Fecire Tunç c. Turquia (de 14 de abril de 2015), *in https://hudoc.echr.coe.int/*.

Acórdão Armani da Silva c. Reino Unido (de 30 de março de 2016), *in https://hudoc.echr.coe.int/*.

Acórdão Khadija Ismayilova c. Azerbaijão (de 10 de janeiro de 2019), *in https://hudoc.echr.coe.int/*.

Acórdão Big Brother Watch e Outros c. Reino Unido (de 25 de maio de 2021), *in https://hudoc.echr.coe.int/*.

Acórdão Volodina c. Rússia (n.º 2) (de 14 de setembro de 2021), *in https://hudoc.echr.coe.int/*.

Tribunal de Justiça da União Europeia

Acórdão Digital Rights Ireland Ltd e Kärntner Landesregierung e Outros (de 8 de abril de 2014, Processos C-293/12 e C-594/12), *in http://curia.europa.eu*.

Acórdão Tele2 Sverige AB e Secretary of State for the Home Department (de 21 de dezembro de 2016, Processos C-203/15 e C-698/15), *in http://curia.europa.eu*.

Acórdão Ministerio Fiscal (de 2 de outubro de 2018, Processo C-207/16), *in http://curia.europa.eu*.

Acórdão Privacy International (de 6 de outubro de 2020, Processo C-623/17), *in http://curia.europa.eu*.

Acórdão La Quadrature du Net e Outros (de 6 de outubro de 2020, Processos C-511/18, C-512/18 e C-520/18), *in http://curia.europa.eu*.

Acórdão Prokuratuur (de 2 de março de 2021, Processo C-746/18), *in http://curia.europa.eu*

Acórdão G. D. e Commissioner of An Garda Síochána (de 5 de abril de 2022, Processo C-140/20), *in http://curia.europa.eu*.

Acórdão SpaceNet e Telekom Deutschland (de 20 de setembro de 2022, Processos C-793/19 e C-794/19), *in http://curia.europa.eu*.

Acórdão A. G. e Lietuvos Respublikos generalinė prokuratūra (de 7 de setembro de 2023, Processo C-162/22), *in http://curia.europa.eu*.

Portugal

Tribunal Constitucional

Acórdão n.º 213/2008, *in www.tribunalconstitucional.pt*.

Acórdão n.º 403/2015, *in www.tribunalconstitucional.pt*.

Acórdão n.º 464/2019, *in www.tribunalconstitucional.pt*.

Acórdão n.º 268/2022, *in www.tribunalconstitucional.pt*.

Supremo Tribunal de Justiça

Acórdão de 3 de março de 2010 (Processo 886/07.8PSLSB.L1.S1), *in www.dgsi.pt*.

Acórdão de 29 de abril de 2010 (Processo 128/05.0JDLSB-A.S1), *in www.dgsi.pt*.

Acórdão de 21 de setembro de 2022 (Processo 79/13.5JBLSB-C.S1), *in www.dgsi.pt*.

Acórdão de 10 de novembro de 2022 (Processo 120/17.2TELSB-B.S1), *in www.dgsi.pt*.

Acórdão de 19 de janeiro de 2023 (Processo 33/15.2JAPRT-B.S1), *in www.dgsi.pt*.

Acórdão de 1 de fevereiro de 2023 (Processo 35/17.4GACHV-A.S1), *in www.dgsi.pt*.

Acórdão de 11 de maio de 2023 (Processo 21/11.8PEPRT-M.S1), *in www.dgsi.pt*.

Acórdão de 21 de junho de 2023 (Processo 1229/19.3TELSB-A.S1), *in www.dgsi.pt*.

Acórdão de 29 de junho de 2023 (Processo 42/10.8PBVCD-B.S1), *in www.dgsi.pt*.

Tribunal da Relação de Coimbra

Acórdão de 17 de maio de 2006 (Processo 1265/06), *in www.dgsi.pt*.

Acórdão de 15 de novembro de 2006 (Processo 915/06.2TAAVR-A.C1), *in www.dgsi.pt*.

Acórdão de 12 de outubro de 2022 (Processo 538/22.9JALRA.C1), *in www.dgsi.pt*.

Acórdão de 21 de junho de 2023 (Processo 302/21.2JACBR.C1), inédito.

Acórdão de 27 de setembro de 2023 (Processo 13/20.6PEVIS.C1), *in www.dgsi.pt*.

Tribunal da Relação de Évora

Acórdão de 26 de junho de 2007 (Processo 843/07-1), *in www.dgsi.pt*.

Acórdão de 25 de outubro de 2022 (Processo 52/18.7GBSLV.E1), *in www.dgsi.pt*.

Acórdão de 28 de fevereiro de 2023 (Processo 661/17.1TELSB.E1), *in www.dgsi.pt*.

Acórdão de 9 de maio de 2023 (Processo 275/22.4GCSTB-A.E1), *in www.dgsi.pt*.

Acórdão de 28 de junho de 2023 (Processo 2010/21.5JFLSB-A.E1), *in www.dgsi.pt*.

Acórdão de 12 de setembro de 2023 (Processo 950/10.6PCSTB.E2), *in www.dgsi.pt*.

Tribunal da Relação de Guimarães

Acórdão de 10 de janeiro de 2005 (Processo 2013/04-1), *in www.dgsi.pt*.

Acórdão de 21 de novembro de 2005 (Processo 1987/05-1), *in www.dgsi.pt*.

Acórdão de 2 de maio de 2023 (Processo 12/23.6 PBGMR-A.G1), *in www.dgsi.pt*.

Tribunal da Relação de Lisboa

Acórdão de 24 de janeiro de 2012 (Processo 35/07.2PJAMD.L1-5), *in www.dgsi.pt*.

Acórdão de 25 de outubro de 2022 (Processo 50/22.6JBLSB-A.L1-5), *in www.dgsi.pt*.

Acórdão de 26 de janeiro de 2023 (Processo 849/20.8PBCSC.L1-9), *in www.dgsi.pt*.

Acórdão de 22 de fevereiro de 2023 (Processo 495/22.1JAFUN-A.L1-5), *in www.dgsi.pt*.

Tribunal da Relação do Porto

Acórdão de 7 de setembro de 2022 (Processo 877/22.9JAPRT-A.P1), *in www.dgsi.pt*.

Acórdão de 7 de dezembro de 2022 (Processo 5011/22.2JAPRT-A.P1), *in www.dgsi.pt*.

Acórdão de 29 de março de 2023 (Processo 47/22.6PEPRT-Z.P1), *in www.dgsi.pt*.

Acórdão de 24 de maio de 2023 (Processo 747/20.5JGLSB.P1), *in www.dgsi.pt*.

Alemanha

Bundesverfassungsgericht

Sentença de 16 de outubro de 1977 (1 BvQ 5/77), *in https://www.bundesverfassungsgericht.de*.

Sentença de 14 de maio de 1985 (1 BvR 233/81; 1 BvR 341/81), *in https://www.servat.unibe.ch/dfr/bv069315.html* (consultado em 30/10/2023).

Sentença de 2 de março de 2010 (1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08), *in https://www.bundesverfassungsgericht.de*.

Sentença de 27 de junho de 2018 (2 BvR 1405/17; 2 BvR 1780/17), *in https://www.bundesverfassungsgericht.de*.

Bundesgerichtshof

Sentença de 24 de janeiro de 2001, *in* Entscheidungen des Bundesgerichtshofes in Strafsachen, 46, pp. 266 e ss., Carl Heymanns Verlag KG, Colónia e Berlim, 2002.

Espanha

Tribunal Supremo

Sentença n.º 6307/2009, *in www.poderjudicial.es*.

Estados Unidos

Supreme Court of the United States

Sentença United States *v.* Jones, *in http://supreme.justia.com* (consultado em 14/10/2023).

United States Court of Appeals

Sentença National City Trading Corp. *v.* United States, 635 F.2d 1020 (2nd Circuit, 1980), *in https://casetext.com/case/national-city-trading-corp-v-united-states-2* (consultado em 14/10/2023).

United States Court for the District of Vermont

Sentença United States *v.* Hunter, 13 F. Supp. 2d 574 (1998), ***in*** *https://law.justia.com/cases/federal/district-courts/FSupp2/13/574/2311683/* (consultado em 14/10/2023).

Direito à Privacidade dos Dados X Segurança Pública – A Invalidação da Diretiva 2006/24/Ce e a Repercução na Legislação Portuguesa

Renata Guilardi de Oliveira Castro[325]

Resumo
O direitos fundamentais à reserva a vida privada e à autodeterminação informacional são resguardados pelo Direito da União Europeia, que, nesse contexto, tutela especificamente a proteção dos dados das pessoas singulares. Assim, as leis dos Estados-membros têm que caminhar nessa mesma direção. Contudo, há situações em que outros direitos fundamentais estão em causa, o que exige ponderação por parte dos tribunais, seja o Tribunal de Justiça da União Europeia ou os tribunais dos Estados-membros, inclusivamente os Tribunais Constitucionais. Assim está a ocorrer em relação a Lei 32/2008, que deve obedecer os parâmetros do TJUE no que tange aos requisitos mínimos de armazenamento de metadados para fins de investigação criminal, situação que exige, dos magistrados envolvidos, muita ponderação para não desconsiderar, indevidamente, nenhum dos direitos fundamentais em causa, quando da aplicação do princípio da proporcionalidade previsto no artigo 52º, n.1 da Carta do Direitos Fundamentais da União Europeia.

Palavras-chaves: Direito da UE, princípio da proporcionalidade, proteção de dados, da vida privada.

[325] Mestranda em Direito Judiciário na Universidade Europeia/Lisboa/Portugal; pós-graduada em Direito Administrativo Contemporâneo pelo Instituto de Direito Administrativo de Goiás/Brasil; formada em Direito pela PUC-Goiás/Brasil.

Right to Data Privacy X Public Security – The Invalidation of Directive 2006/24/Ec and the Repercussion on Portuguese Legislation

Renata Guilardi de Oliveira Castro

Abstract
The fundamental rights to privacy and informational self-determination are protected by European Union Law, which, in this context, specifically protects the protection of natural persons' data. Therefore, the laws of the Member States must move in the same direction. However, there are situations in which other fundamental rights are at stake, which require consideration by the courts, whether the Court of Justice of the European Union or the courts of the Member States, including the Constitutional Courts. This is what is happening in relation to Law 32/2008, which must comply with the CJEU's parameters regarding the minimum requirements for storing metadata for the purposes of criminal investigation, a situation that requires, from the magistrates involved, a lot of consideration so as not to unduly disregard , none of the fundamental rights in question, when applying the principle of proportionality provided for in article 52, n.1 of the Charter of Fundamental Rights of the European Union.

Keywords: EU law, principle of proportionality, data protection, privacy.

Introdução

Como direitos fundamentais, a reserva da intimidade da vida privada e a autodeterminação informacional não podem sofrer ingerências injustificadas e/ou desproporcionais.

No sentido de garantir a segurança contra crimes graves, dentre eles o terrorismo, foi publicada a Diretiva 2006/24/CE, cujo objetivo era uniformizar as legislações dos Estados-membros da União Europeia no que diz respeito ao armazenamento dos dados/metadados dos cidadãos para eventuais investigações criminais. Assim, foi dada abertura para a flexibilização dos direitos fundamentais acima mencionados, quando estritamentente necessária para salvaguardar outro direito fundamental: a segurança.

Contudo, o Tribunal de Justiça da União Europeia - TJUE, em 2014, analisando dois casos de reenvio prejudicial (Processo C-293/12 e Processo C-594/12), declarou a invalidade dessa Diretiva por considerar que, apesar das medidas serem pertinentes aos objetivos da Diretiva (combate a crimes graves), a abrangência e generalidade das ingerências aos direitos à vida privada e à autodeterminação informacional dos cidadãos eram desproporcionais ao fim almejado.

Em Portugal, a decisão do TJEU não foi imediatamente aplicada à Lei 32/2008, de 17 de julho, que transpôs, para o ordenamento jurídico Português, aquela Diretiva 2006/24/CE, ou seja, a Lei continuou em vigor, correndo o risco de lesar direitos fundamentais.

Somente em 2022, através de um controlo abstrato da constitucionalidade, o Tribunal Constitucional de Portugal retirou do ordenamento jurídico interno os dispositivos que lesavam a reserva da intimidade da vida privada e a autodeterminação informacional. Ressalta-se que o Acórdão 268/2022 do Tribunal Constitucional de Portugal, ao declarar a inconstitucionalidade dos artigos 4.º, 6.º e, parcialmente, do artigo 9.º, todos da Lei 32/2208, o fez por serem diretamente incompatíveis com os números 1 e 4 do artigo 35.º; n.º 1 do artigo 26.º e o n.º 2 do artigo n.º 18.º, todos da Constituição da República Portuguesa – CRP, sendo que a compatibilidade com o direito eurocomunitário foi vista indiretamente.

Percebe-se que a declaração de invalidade da Diretiva não foi aplicada diretamente em relação à Lei 32/2008.

A primeira questão que se faz é sobre a aplicação do princípio do primado do direito eurocomunitário em casos como esse, onde a Diretiva que ensejou a

promulgação da lei é declarada inválida. Como a decisão decorreu do julgamento de dois casos de reenvio pré-judicial, deveria repercutir apenas nos processos C-293/12 e C-594/12 ou nas legislações de transposição de todos os Estados-membros?

Da análise dos acórdãos do Tribunal de Justiça da União Europeia e do Tribunal Constitucional de Portugal se constata a atual relevância dos direitos à reserva da intimidade da vida privada e à autodeterminação informacional. Nota-se a evolução do primeiro e a construção do segundo no sentido de assegurar a proteção dos dados das pessoas, em que pese não exista ainda uma plena conscientização, entre os destinatários dessa proteção, sobre a importância de resguardar os dados, sejam de identificação, tráfego ou localização, tanto é que a o acórdão 268/2022 do Tribunal Constitucional de Portugal foi objeto de imensas críticas, inclusivamente por parte de autoridades, que colocaram em causa o combate à criminalidade grave, que seria prejudicado por essa demasiada proteção, já que o acesso a esses dados são uma forma eficaz de se obter provas para instruir processos criminais.

Portanto, a segunda questão que se faz versa sobre a aplicação do princípio da proporcionalidade ou ponderação, quando do conflito entre direitos fundamentais, no caso, entre a proteção dos dados das pessoas singulares e coletivas (direito a privacidade e autodeterminação informacional) X a segurança pública.

A importância desse estudo é tentar apontar respostas a essas questões pertinentes e atuais, através da metodologia de pesquisa bibliográfica em livros científicos, artigos científicos e legislação.

Para tanto, no capítulo 1 será abordada a natureza jurídica do direito à privacidade e do direito à proteção dos dados pessoais para termos uma noção da importância da proteção dos dados no contexto contemporâneo.

No segundo capítulo será analisada a Directiva 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e sua declaração de invalidade pelo Tribunal de Justiça da União Europeia - TJUE. A importância dessa análise, para o presente trabalho, é aferir como o TJUE interpreta os direitos à reserva a vida privada e à autodeterminação informacional e a densificação que lhes são conferidos num contexto de conflito

com o direito à seguraça pública (combate à criminalidade grave), à luz do princípio da ponderação.

No terceiro capítulo os efeitos desse acórdão do TJUE sobre a legislação de Portugal serão tratados, havendo a subdivisão do capítulo em três partes. Na primeira, será analisado se aquele acórdão deveria, ou não, vincular o direito interno de Portugal à luz do princípio do primado do direito da União Europeia. Na segunda parte, será analisado como o Tribunal Constitucional de Portugal analisou a questão, conforme o Acórdão 268/2022. Diante da declaração de inconstitucionalidade de alguns artigos da Lei 32/2008, através desse Acórdão 268/2022, a Assembleia da Republica teve que elaborar alterações nessa Lei a fim de adequá-la à interpretação conferida à reserva a vida privada e à autodeterminação informacional conferida pelo Tribunal Constitucional de Portugal e pelo Tribunal de Justiça da União Eurpeia, razão pela qual nasceu o Decreto n.º 91/XV, de 26 de outubro de 2023, que não passou pelo crivo de constitucionalidade do Tribunal Constitucional de Portugal em processo de fiscalização preventiva da constitucionalidade. Assim, os motivos desse veto serão analisados.

Ao final, poderemos ter uma visão crítica dessa questão tão pertinente.

1- Natureza jurídica do direito à privacidade e do direito à proteção dos dados pessoais

O direito à privacidade segundo Warren e Brandeis, em 1890,[326] foi concebido como uma necessidade decorrente das mudanças políticas, sociais e econômicas da época, sendo essa evolução legislativa natural e necessária diante das "invenções recentes e métodos de negócios", como fotografias instantâneas e empresas jornalísticas, que traziam novas perspectivas de lesões e clamavam, consequentemente, por novas perspectivas dos direitos já reconhecidos (lei da difamação e lei da literatura e propriedade artística). Nesse sentido nasceu o direito de "ser deixado em paz", no sentido de resguardar a vida privada do indivíduo contra publicações sem o seu consentimento, que poderiam expor sua intimidade e causar danos, independentemente de serem verdadeiras ou não, danos que foram estendidos do aspecto físico para os danos psicológicos e à imagem.

[326] Warren e Brandeis, "O Direito à Privacidade" (mit.edu)

Após a 2ª Guerra Mundial a pessoa passou a ser o centro do ordenamento jurídico. Desde a Declaração Universal dos Direitos do Homem, de 1948, o Princípio da Dignidade da Pessoa Humana vem se tornando um princípio jurídico fundamental que transcende ao ordenamento jurídico positivado dos países que o assumiram como origem, exercendo uma função "normogenética" na medida em que fundamenta as regras e princípios do ordenamento jurídico constituindo a sua *ratio*, bem como se torna fonte criadora de novas normas, ou seja, esse princípio é a raiz ética dos direitos fundamentais:[327] "a humanidade compreendeu, mais do que em qualquer outra época da História, o valor supremo da dignidade humana" (COMPARATO, Fábio Konder. 2003, p. 68).

Nesse contexto, o direito à privacidade ganhou força, como se observa da Declaração Universal dos Direitos do Homem, que prevê, no seu artigo 12: *Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.*

A Organização das Nações Unidas apenas implementou o artigo 12 da Declaração Universal dos Direitos do Homem (acima citado), ao adotar, em 2013, duas resoluções sobre "o direito à vida privada na era digital" visando proteger o indivíduo da vigilância em larga escala e, em 2016 e 2017, foram adotadas outras resoluções nesse sentido, pois "as capacidades crescentes das empresas para recolher, tratar e utilizar dados pessoais podem representar um risco para o gozo do direito à privacidade na era digital."

Apesar de não mencionar, especificamente, o direito à proteção de dados como um direito autônomo, essas resoluções revelam que a ONU não está à margem desse novo conceito de vida privada (direito a autodeterminação informacional) e, além da responsabilidade das autoridades públicas, assinala a responsabilidade do setor privado na proteção dos direitos humanos quando lidarem com informações pessoais, sendo um contributo para a regulamentação interna dos países signatários.

A consolidação do direito à privacidade à luz do princípio da Dignidade da Pessoa Humana, ao longo dos anos, foi e está sendo determinante para nortear o

[327] O Recurso ao Princípio da Dignidade da Pessoa Humana na Jurisprudência do Tribunal Constitucional – Benedita Mac Crorie

legislador contemporâneo no sentido de tentar perceber e evitar os riscos de lesão à privacidade do homem no contexto do mundo digital.

A pessoa, nessa nova perspectiva, engloba tanto ao seu corpo físico quanto o corpo eletrônico (conjunto dos seus dados). Esse corpo eletrônico foge da esfera de disponibilidade do titular quando ele fornece informações pessoais que são armazenadas por terceiros. Quando essas informações são utilizadas indevidamente, sem o consentimento do indivíduo fornecedor da informação, acaba por desapropriá-lo de sua autonomia visto que não mais detém o controlo do seu patrimônio informativo, do seu corpo eletrônico que agora pode ser disseminado.

A nova sociedade, cada vez mais dependente da internet, exigiu uma nova perspectiva sobre o conceito de privacidade. O conceito de privacidade, no sentido de ser privado da exposição pública, vai abandonando a qualificação de "secreto" para ganhar a conotação de "pessoal", sendo um dos vários aspectos desse novo conceito a manutenção do controlo quanto ao tratamento e utilização dos seus dados disponibilizados em rede, ou seja, há a necessidade de um meio ambiente digital seguro, onde o controlo de dados pessoais sob a égide da proteção estatal viabilize a autodeterminação informativa, onde cada qual figure com poderes reais sobre suas informações e dados. Assim, os ideais da atual noção de privacidade estão em encontrar formas seguras de circulação das informações e não mais em impedir o andamento delas. Rodotà (2008) defende uma reinterpretação do conceito de privacidade, enriquecendo a definição tradicional como "direito de ficar só" com o direito à autodeterminação informacional, conceito que engloba o direito de manter o controle sobre as próprias informações; o direito de escolher aquilo que será revelado; o direito ao esquecimento, em resumo, o direito de determinar a maneira de construir a própria esfera particular, impedindo-se que a pessoa se transforme em objeto de informação. O autor explica que enquanto expressão da dignidade, a proteção dos dados contribui para a "constitucionalização da pessoa" que deve poder ter o controle integral dos seus dados para desenvolver livremente sua personalidade.

Assim, apesar da estreita ligação, o direito ao respeito pela vida privada e o direito à proteção aos dados pessoais são direitos distintos, até porque aquele foi declarado muito antes da existência dos computadores e da internet, tecnologias que trouxeram mudanças políticas, sociais e econômicas e provocaram um novo

conceito de vida privada (direito a autodeterminação informacional), que levou ao desenvolvimento de normas legais especiais, mais adequados às especificidades do mundo digital.

Na Europa, a Convenção Europeia dos Direitos do Homem (CEDH), de 1950, também consagra o direito à vida privada, no seu artigo 8º:

> *Direito ao respeito pela vida privada e familiar*
> *1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.*
> *2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.*

A Convenção de Strasbourg nº 108 do Conselho Europeu (1981), que entrou em vigor em 1985, foi redigida com a intenção de unificar e regulamentar a proteção de dados pessoais, sendo vinculativa para os Estados que a ratificaram, embora não esteja sujeita à fiscalização judicial do Tribunal Europeu dos Direitos Humanos. Vale ressaltar que todos os Estados-Membros da União Europeia ratificaram.

Na Carta dos Direitos Fundamentais da União Europeia (CARTA), de dezembro de 2000, o artigo 7º corresponde ao direito à vida privada: *Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.* E, no artigo 8º, consagra o direito à proteção de dados:

> *Protecção de dados pessoais*
> *1. Todas as pessoas têm direito à protecção dos dados de caráter pessoal que lhes digam respeito.*
> *2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.*
> *3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.*

Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia reconhecem o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais estreitamente relacionados, mas distintos. Ambos visam proteger a autonomia e a dignidade humana dos indivíduos, assegurando-lhes uma

esfera pessoal no âmbito da qual possam livremente desenvolver as suas personalidades, pensar e formar as suas opiniões, mas diferem na formulação e no alcance.

O direito à vida privada visa proibir a ingerência injustificada na vida privada do indivíduo, já a proteção de dados é um direito ativo que estabelece um sistema para proteger o indivíduo sempre que os seus dados pessoais são tratados. A proteção de dados refere-se a todos os tipos de dados pessoais e de tratamento dos dados, independentemente da relação e do impacto sobre a vida privada, ou seja, para aplicar as regras sobre proteção de dados não é necessário que ocorra uma ingerência na vida privada (que pode ocorrer) - Manual da Legislação Europeia sobre Proteção de Dados.

Ao ser proclamado na Carta dos Direitos Fundamentais da União Europeia, o direito à proteção de dados passou a ser um direito fundamental e foi incorporado nos princípios gerais de direito europeu, nos termos do artigo 52º, n. 1, da própria Carta:

> *Artigo 52.o*
> *Âmbito e interpretação dos direitos e dos princípios*
> *1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.*

Esse documento se tornou juridicamente vinculativo com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009, nos termos do seu artigo 6.º, n.º 1. [328], bem como no Tratado sobre o Funcionamento da União Europeia, artigo 16º, n.1.[329]

---

[328] ARTIGO 6º

1. A união reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, e que tem o mesmo valor jurídico que os Tratados. De forma alguma o disposto na Carta pode alargar as competências da União, tal como definidas nos Tratados.

[329] ARTIGO 16º

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Sendo Portugal um Estado-membro desde 1986, ele teve que adequar sua legislação aos princípios da vida privada e da proteção de dados. Ressalta-se que a Constituição da República Portuguesa, no Título II da Parte I (Direitos e deveres fundamentais), prevê o direito à utilização da informática, o que inclui o direito à proteção de dados e, em 17 de maio de 2021, proclamou a Carta Portuguesa de Direitos Humanos na Era Digital, que prevê, no artigo 8º, o Direito à privacidade em ambiente digital.[330]

Portanto, a natureza jurídica da proteção de dados é de direito fundamental do homem, pois previsto nas convenções internacionais, bem como direito fundamental por também estar previsto na Constituição da República Portuguesa. Esse princípio é inerente à própria dignidade da pessoa humana, que é um conceito em crescente processo de evolução e desenvolvimento, princípio que fundamenta a Constituição da República Portuguesa (artigo 1º) em consonância com a Declaração de Universal dos Direitos do Homem.

2. Directiva 2006/24/CE e sua declaração de invalidade pelo Tribunal de Justiça Europeu

O Parlamento Europeu e o Conselho da União Europeia, tendo em conta a proposta da Comissão e o parecer do Comité Económico e Social, adotaram a Diretiva 95/46/CE de 24 de Outubro de 1995[331], relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que exigia que os Estados-Membros garantissem os direitos e liberdades das pessoas singulares no que respeita ao tratamento de dados pessoais, nomeadamente o seu

[330] Direito à privacidade em ambiente digital

1 - Todos têm direito a comunicar eletronicamente usando a criptografia e outras formas de proteção da identidade ou que evitem a recolha de dados pessoais, designadamente para exercer liberdades civis e políticas sem censura ou discriminação.

2 - O direito à proteção de dados pessoais, incluindo o controlo sobre a sua recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, é assegurado nos termos legais.

[331] O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, revogou a Diretiva 95/46/UE ao dispor sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

direito à privacidade, com o objetivo de assegurar a livre circulação de dados pessoais na Comunidade.

Esse documento, que foi o primeiro instrumento sobre proteção de dados da União Europeia, sendo anterior à Carta dos Direitos Fundamentais da União Europeia, inclusive, permitia que os Estados-Membros adotassem medidas legislativas para restringir a privacidade e o respeito ao tratamento desses dados pessoais quando tal providência fosse necessária para salvaguardar a prevenção, investigação, deteção e repressão de infrações penais.[332]

Complementando, sobreveio a Directiva 97/66/CE, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações. Esta Directiva foi substituída pela Directiva 2002/58/CE, de 12 de Julho de 2002, a fim de adaptar-se ao desenvolvimento dos mercados e das tecnologias dos serviços de comunicações electrónicas, de modo a proporcionar um nível idêntico de proteção dos dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas.

Alterando a Directiva 2002/58/CE, foi publicada, em 15 de março de 2006, a Directiva 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente

---

[332] Artigo 13

Isenções e restrições

1. Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito das obrigações e direitos previstos nos artigos 6.º, n.º 1, 10.º, 11.º, n.º 1, 12.º e 21.º, quando tal restrição constitua uma medida necessária para salvaguardar:

(a) segurança nacional;

(b) defesa;

(c) segurança pública;

(d) a prevenção, investigação, deteção e repressão de infrações penais ou de violações da ética em profissões regulamentadas;

(e) Um interesse económico ou financeiro importante de um Estado membro ou da União Europeia, incluindo questões monetárias, orçamentais e fiscais;

(f) uma função de fiscalização, fiscalização ou regulação relacionada, ainda que pontualmente, com o exercício da autoridade pública nos casos referidos nas alíneas (c), (d) e (e);

(g) a proteção do titular dos dados ou dos direitos e liberdades de terceiros.

disponíveis ou de redes públicas de comunicações. Seu principal objetivo era harmonizar as legislações nacionais no que tange ao armazenamento e disponibilização dos dados das pessoas singulares e coletivas, para a finalidade de investigação criminal. Para tanto, traçou alguns parâmetros como o tempo de armazenamento dos dados (entre 6 meses e 02 anos) e as informações que teriam que ficar armazenadas à disposição das autoridades: dados de tráfego e de localização, bem como os dados conexos necessários para identificar o assinante ou os utilizados dos serviços de comunicações eletrônicas.

Obedecendo o dever de transpor a Diretiva 2006/24/CE para o seu ordenamento interno, vários Estados-membros publicaram normas, sendo que algumas foram objeto de questionamentos perante os seus respectivos Tribunais, ensejando o reenvio prejudicial previsto no artigo 267º do Tratado sobre o Funcionamento da União Europeia.

A transposição dessa Directiva do Parlamento Europeu e do Conselho Europeu, para o ordenamento jurídico de Portugal, foi através da Lei n. 32/2008 de 17 de julho[333].

Dois pedidos de decisão prejudicial foram analisados pelo Tribunal de Justiça da União Europeia em **08 de abril de 2014**, tendo como objeto da validade da Diretiva 2006/24/CE.

Em 11/08/2006 a empresa Digital Rights interpôs um recurso perante a High Court alegando que é proprietária e utilizadora de um telemóvel desde junho de 2006 e que a conservação dos dados de suas comunicações telefónicas, no que tange ao tráfego e à localização, por determinado tempo, com o objetivo de

[333] Artigo 1.º - Objecto

1 - A presente lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

2 - A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações.

prevenção e detenção das infrações terroristas, investigação e repressão das mesmas, a fim de garantir a segurança do Estado, como prevê a Lei de 2005, que transpôs a Diretiva 2006/24, lesava o seu direito à privacidade.

A High Court suspendeu a instância e submeteu, ao Tribunal Europeu, a questão prejudicial acerca da validade da Diretiva 2006/24, através do Processo C-293/12, por entender ser que essa questão era a causa de pedir indireta, formulando as seguintes questões prejudiciais:

> *1) A restrição dos direitos da "recorrente", no que respeita à utilização da rede telefónica móvel, resultante das exigências dos artigos 3.°, 4.° e 6.° da Diretiva 2006/24/CE é incompatível com o artigo 5.°, n.° 4, TUE, na medida em que é desproporcionada e desnecessária ou inadequada para alcançar os objetivos legítimos de:*
> *a) assegurar que determinados dados são disponibilizados para efeitos de investigação, deteção e repressão de crimes graves?*
> *e/ou*
> *b) assegurar o funcionamento adequado do mercado interno da União Europeia?*
> *2) Concretamente,*
> *a) A Diretiva 2006/24/CE é compatível com o direito dos cidadãos de circularem e permanecerem livremente no território dos Estados-Membros, consagrado no artigo 21.° TFUE?*
> *b) A Diretiva 2006/24/CE é compatível com o direito ao respeito pela vida privada, consagrado no artigo 7.° da Carta [dos Direitos Fundamentais da União Europeia (a seguir 'Carta')] e no artigo 8.° da CEDH?*
> *c) A Diretiva 2006/24/CE é compatível com o direito à proteção dos dados pessoais, consagrado no artigo 8.° da Carta?*
> *d) A Diretiva 2006/24/CE é compatível com o direito à liberdade de expressão, consagrado no artigo 11.° da Carta e no artigo 10.° da CEDH?*
> *e) A Diretiva 2006/24/CE é compatível com o direito a uma boa administração, consagrado no artigo 41.° da Carta?*
> *3) Em que medida os Tratados — e, em concreto, o princípio da cooperação leal previsto no artigo 4.°, n.° 3, TUE — exigem que os tribunais investiguem e apreciem a compatibilidade das medidas nacionais de transposição da Diretiva 2006/24/CE com as garantias conferidas pela [Carta], incluindo o seu artigo 7.° (cujo conteúdo é inspirado no artigo 8.° da CEDH)?»*

Também foi objeto de análise o processo C-594/12, decorrente de recursos interpostos no Verfassungsgerichtshof (Tribunal Constitucional Autríaco), respetivamente, pela Kärntner Landesregierung e por M. Seitlinger, C. Tschohl e tantos outros recorrentes, que pediam a anulação do artigo 102.°-A da Lei de 2003, sobre as telecomunicações, inserido nesta lei pela lei de alteração BGBl. I, 27/2011, para efeitos da transposição da Diretiva 2006/24 para o direito interno austríaco.

A alegação era que o artigo 102.°-A supra mencionado violava o direito fundamental dos particulares à proteção dos seus dados, tendo, o

Verfassungsgerichtshof, questionado se a Diretiva 2006/24 era compatível com a Carta na medida em que permitia o armazenamento de um volume de tipos de dados relativos a um número ilimitado de pessoas durante um longo período, cujo comportamento não justifica sequer que os seus dados sejam conservados, deixando-as expostas a um risco superior de que as autoridades investiguem os seus dados, tomassem conhecimento do seu conteúdo, se informassem acerca da sua vida privada e utilizassem estes dados com múltiplas finalidades, tendo designadamente em conta o número incomensurável de pessoas que tinham acesso aos dados durante um período de, pelo menos, seis meses.

Segundo o órgão jurisdicional de reenvio, havia dúvidas, por um lado, quanto ao facto de esta diretiva poder alcançar os seus objetivos e, por outro, quanto ao caráter proporcionado da ingerência nos direitos fundamentais em causa. Nestas condições, foram submetidas ao Tribunal de Justiça as seguintes questões prejudiciais:

> *«1) Quanto à validade dos atos adotados pelas instituições da União: Os artigos 3.° a 9.° da Diretiva [2006/24] são compatíveis com os artigos 7.°, 8.° e 11.° da [Carta]?*
> *2) Quanto à interpretação dos Tratados:*
> *a) À luz das anotações ao artigo 8.° da Carta, as quais, nos termos do artigo 52.°, n.° 7, da Carta, devem ser tidas em devida conta pelo Verfassungsgerichtshof como orientações para a interpretação da referida Carta, a Diretiva [95/46] e o Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados [(JO 2001, L 8, p. 1)], devem ser tidos em consideração de forma equivalente às condições constantes do artigo 8.°, n.° 2, e do artigo 52.°, n.° 1, da Carta, ao apreciar a admissibilidade das ingerências?*
> *b) Qual é a relação existente entre o 'direito da União', referido na última frase do artigo 52.°, n.° 3, da Carta, e as diretivas em matéria do direito à proteção de dados?*
> *c) Atendendo ao facto de a Diretiva [95/46] e o Regulamento [...] n.° 45/2001 imporem condições e restrições na salvaguarda do direito fundamental à proteção de dados constante da Carta, as alterações resultantes do direito derivado posterior devem ser tidas em consideração ao interpretar o artigo 8.° da Carta?*
> *d) Considerando o artigo 52.°, n.° 4, da Carta, resulta do princípio da salvaguarda de um nível de proteção mais elevado, consagrado no artigo 53.° da Carta, que os limites, estabelecidos pela Carta, para as restrições que podem ser colocadas pelo direito derivado devem ser definidos de acordo com critérios mais exigentes?*
> *e) Considerando o artigo 52.°, n.° 3, da Carta, o artigo 5.° do preâmbulo e as anotações ao artigo 7.° da Carta, nos termos das quais os direitos aí garantidos correspondem aos direitos garantidos*

pelo artigo 8.° da CEDH, é possível deduzir da jurisprudência do Tribunal Europeu dos Direitos do Homem em relação ao artigo 8.° da CEDH a existência de elementos de interpretação do artigo 8.° da Carta que possam influenciar a interpretação deste último artigo?»

Por decisão do presidente do Tribunal de Justiça, os processos C-293/12 e C-594/12 foram apensados para efeitos da fase oral e do acórdão, cujo conteúdo foi o seguinte:

Sobre o direito à liberdade de expressão, consagrado no artigo 11.° da Carta e no artigo 10.° da CEDH, o TJ considerou que os dados a serem conservados possibilitam encontrar e identificar a fonte e o destino de uma comunicação, determinado a data, a hora, a duração e o tipo de uma comunicação; o equipamento de comunicação dos utilizadores, bem como a localização do equipamento de comunicação móvel; o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços Internet, ou seja, possibilitam saber qual é a pessoa com quem um assinante ou um utilizador registado se comunicou e com que frequência e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Através desses dados pode-se descobrir aspectos pormenorizados da vida privada da pessoa, o que fere a liberdade de expressão da pessoa, mesmo sem o armazenamento do conteúdo das comunicações e das informações consultadas.

Sobre o respeito pela vida privada e o direito à proteção dos dados pessoais, consagrados nos artigos 7.° e 8º da Carta dos Direitos Fundamentais da União Europeia (CARTA) e artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH), foi decidido que quando os dados são conservados por determinado tempo, como determina a Diretiva 2006/24/CE, há a derrogação do regime de proteção do direito ao respeito da vida privada, instituído pelas Diretivas 95/46/CE e 2002/58/CE, visto que estas diretivas consagram a confidencialidade das comunicações e dos dados relativos ao tráfego, bem como a obrigação de eliminar ou de tornar anónimos esses dados, quando deixem de ser necessários para a transmissão de uma comunicação e faturação. Portanto, há uma ingerência no direito fundamental ao respeito da vida privada, independentemente dessas informações versarem, ou não, sobre caráter sensível, ou que os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência.

Além disso, o acesso das autoridades nacionais competentes aos dados, como permitem os artigos 4.º e 8.º da Diretiva 2006/24/CE, constitui uma ingerência suplementar neste direito fundamental e o facto de a conservação dos dados e a sua utilização posterior serem efetuadas sem que o assinante ou o utilizador registado sejam informados disso é suscetível de gerar no espírito das pessoas em causa, a sensação de que a sua vida privada é constantemente vigiada.

Quanto à questão de saber se a referida ingerência respondia a um objetivo de interesse geral da União, a resposta foi sim, pois o objetivo material desta diretiva era contribuir para a luta contra a criminalidade grave e, assim, em última análise, para a segurança pública, decorrente da necessidade de lutar contra o terrorismo internacional, com vista à manutenção da paz e da segurança internacionais. Além disso, importa salientar, a este respeito, que o artigo 6.º da Carta enuncia o direito das pessoas não só à liberdade mas também à segurança.

A este respeito, o Conselho «Justiça e Assuntos Internos» de 19 de dezembro de 2002 considerou que os dados gerados pela utilização desse tipo de comunicações são extremamente importantes e constituem, portanto, um instrumento útil na prevenção das infrações e na luta contra a criminalidade, designadamente a criminalidade organizada, fundamento do considerando 7 da Diretiva 2006/24/CE.

Diante do aparente conflito entre direitos fundamentais (o importante papel desempenhado pela proteção dos dados pessoais na perspectiva do direito fundamental ao respeito da vida privada X a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, em prol do direito à segurança), foi aplicado o princípio da proporcionalidade, a fim de aferir a justificação da ingerência nos direitos garantidos pelos artigos 7.º e 8.º da Carta, como prevê o artigo 52º. nº. 1 desse mesmo diploma, que exige, segundo o Tribunal, *que os atos das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos* (v., neste sentido, acórdãos Afton Chemical, C-343/09, EU:C:2010:419, n.º 45; Volker und Markus Schecke e Eifert, EU:C:2010:662, n.º 74; Nelson e o., C-581/10 e C-629/10, EU:C:2012:657, n.º 71; Sky Österreich, C-283/11, EU:C:2013:28, n.º 50; e Schaible, C-101/12, EU:C:2013:661, n.º 29 *apud* Acórdão ECLI:EU:C:2014:238).

Em que pese a conservação desses dados pode ser considerada adequada à realização do objetivo prosseguido pela dita Diretiva, pois a eficácia da luta contra a criminalidade grave pode depender da utilização das técnicas modernas de investigação, o TJUE entendeu que esse motivo não justificava, por si só, a amplitude e a gravidade da ingerência aos princípios da proteção de dados e da vida privada, pois a proteção da vida privada exige, em quaisquer circunstâncias, que as derrogações à proteção dos dados pessoais e as suas limitações ocorram na estrita medida do necessário, razão pela qual a regulamentação da União deveria ter estabelecido regras claras e precisas, impondo exigências mínimas, de modo a que as pessoas cujos dados fossem conservados dispusessem de garantias suficientes na proteção dos seus dados pessoais contra os riscos de abuso e de qualquer acesso e utilização ilícita dos mesmos.

Mas a Diretiva 2006/24/CE abrangia, de maneira geral, todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves, pois não exigia nenhuma relação entre os dados a serem conservados e uma real ameaça para a segurança pública. Assim, visava todos os meios de comunicação eletrónica (cada vez mais importantes na vida quotidiana de todos). Além disso, em conformidade com o seu artigo 3.º, a referida diretiva abrangia todos os assinantes e utilizadores registados. Comportava, portanto, uma ingerência nos direitos fundamentais de quase toda a população europeia.

Por sua vez, também não estabelecia critérios objetivos (condições materiais e processuais) que permitiam delimitar o acesso das autoridades nacionais competentes aos dados e a sua posterior utilização no combate às infrações graves, para justificar a amplitude e a gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta. Ou seja, não estipulava um controlo prévio a ser efetuado por um órgão jurisdicional ou por uma entidade administrativa independente a fim de limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido, acesso condicionado a um pedido fundamentado destas autoridades, apresentado no âmbito de procedimentos de prevenção, de deteção ou de uma ação penal. Também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais limitações.

No que tange à duração da conservação dos dados, a Diretiva 2006/24/CE determinava, no seu artigo 6.°, que fossem conservados entre seis e vinte e quatro meses, sem impor nenhum critério ou distinção entre as categorias de dados previstas no artigo 5.° desta diretiva em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa.

Portanto, ao não estabelecer regras claras acerca do alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta, não resguardava as pessoas porque não prevê garantias suficientes às quais os Estados-membros devem observar para que essa ingerência se limite efetivamente ao estritamente necessário.

Assim, o Tribunal decidiu que o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da Carta, sendo, a Diretiva 2006/24/CE, inválida.

3- Efeitos desse acórdão do Tribunal de Justiça Europeu na legislação de Portugal

3.1- Princípio da Primado do direito da União Europeia

Não se pode afirmar que existe uma "Constituição Supranacional", pois os Estados-membros têm suas próprias Constituições, sendo, a função conformadora dos Tratados e o conteúdo das normas de direito derivado, dependentes do pacto que esses Estados fizerem.

Assim, a autonomia da ordem jurídica da União Europeia decorre das competências que lhe foram atribuídas pelos Estados-membros, o que confere legitimidade ao princípio do primado ou da primazia do direito eurocomunitário, que determina que, em caso de conflito, os Estados têm o dever de aplicar a norma de direito da União Europeia e de desaplicar a norma de direito nacional.

Segundo Pierre Pescatore, *apud* DUARTE, Maria Luíza, 2021, p. 333, o primado é a "*exigência existencial*" do Direito Comunitário e, conforme fundamentação do Tribunal de Justiça da União Europeia, no acórdão de 15/07/1964, do julgamento do caso Costa c. Enel, "*os termos e o espírito do Tratado têm por corolário a impossibilidade, para os Estados, de fazerem prevalecer, sobre uma ordem jurídica*

por todos aceite numa base de reciprocidade, uma medida unilateral posterior que não se lhe pode opor".

A autoridade da jurisprudência do Tribunal de Justiça da União Europeia é importante para garantir a coalização dos Estados-membros e a "força" da União Europeia, e vem sendo construída ao longo dos anos, baseada no princípio da "interpretação conforme na medida do possível", que é inerente ao sistema do Tratado, na medida em que permite ao juiz nacional assegurar, no âmbito de sua competência, a plena eficácia do direito da União (acórdão de 05/10/2004, C-397 a C-403/01, Pfeiffer, nº. 114).

Assim, a consequência operativa do princípio do primado é o afastamento ou desaplicação da norma interna contrária, ou seja, depois de esgotadas as metodologias de sanar o conflito entre a norma eurocomunitária e a norma interna aparentemente contrária, aplicando o princípio da "interpretação conforme na medida do possível" e, se não for eficaz para manter a norma interna, pode o juiz nacional ou o juiz do TJUE aplicar o princípio do primado. No caso *Simmenthal* (acórdão de 09.03.1978), o TJUE considerou que a norma interna contrária é inaplicável de pleno direito, desde o momento da sua entrada em vigor.

Corroborando esse entendimento, há o artigo 4º, nº. 3, do TUE, do qual decorre o princípio da cooperação leal: *Em virtude do princípio da cooperação leal, a União e os Estados-membros respeitam-se e assistem-se mutuamente no cumprimento dos Tratados ou resultantes dos atos das instituições dos Tratados.*

Conclui-se que a lei interna, de transposição de uma Diretiva, deve ser interpretada à luz do texto e da finalidade da Diretiva, mas, e quando essa Diretiva é declarada inválida, o que ocorre com a lei interna?

Em que pese a Diretiva 2006/24/CE tenha sido declarada inválida pelo Tribunal de Justiça da União Europeia em 2014, a Lei 32/2008 de Portugal, que a transcreveu para o ordenamento jurídico interno, continuou em vigor por 08 anos, tendo sido sua constitucionalidade analisada somente em 2022, pelo Tribunal Constitucional de Portugal (Acórdão 268/2022).

No próprio requerimento da Provedora de Justiça, a fim de justificar a competência da jurisdição nacional para a análise do pedido de declaração de inconstitucionalidade dos artigos 4º, 6º e 9º da Lei 32/2008, ela considerou que esta Lei não é "uma ação inteiramente determinada pelo Direito da União" (Acórdão 268/2022, nº 20), em que pese tenha reconhecido que, por ser a transposição para

a ordem jurídica nacional da Directiva 2006/24/CE do Parlamento Europeu e do Conselho, a Lei estava vinculada à Carta dos Direitos Fundamentais da União Europeia (CARTA) e se enquadrava no âmbito de aplicação do direito da União, no termos do disposto no n.º 1 do artigo 51.º da CARTA (itens 17 e 18 do Acórdão).

Esses argumentos parecem contraditórios, pois se a Lei 32/2008 estava vinculada à CARTA e a Diretiva 2006/24/CE foi declarada inválida justamente por lesar princípios assegurados pela CARTA, por qual motivo a Lei não foi considerada "uma ação inteiramente determinada pelo direito da União"?

No acórdão do Tribunal Constitucional de Portugal, este órgão considerou que não estava em causa a aplicação do princípio do primado do Direito da União Europeia, que poderia ser aplicado pelos juízes e tribunais ordinários, nos casos concretos, a fim de desaplicar a Lei 32/2008, mas que, estava em causa, a apreciação da validade de uma norma jurídica nacional (*in abstrato),* não sendo o Direito da União Europeia o foco direto, mas a Constituição, em cuja interpretação deveria intervir o Direito da União Europeia, mais precisamente, os princípio da CARTA. Assim, concluiu que

> "a incompatibilidade de certa norma nacional com o direito da União Europeia não implica, de forma automática, um juízo de inconstitucionalidade; provoca, ao invés, uma afetação da sua eficácia no plano interno, na medida em que contradiga regras europeias simultaneamente mobilizáveis."

Ressalta-se que um dos argumentos do requerimento da Provedora de Justiça perante o Tribunal Constitucional de Portugal foi que, com base no acórdão do TJUE, de 08 de abril de 2014, a Comissão Nacional de Proteção de Dados (CNPD) emitiu a Deliberação n.º 641/2017, considerando que a Lei n.º 32/2008 "*contém normas que prevêem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e pelas comunicações e à protecção dos dados pessoais com grande amplitude e intensidade, em violação do princípio da proporcionalidade e, portanto, em violação do n.º 1 do artigo 52.º da Carta, bem como uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à protecção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa*" e,

através da Deliberação n.º 1008/2017, de 18 de julho, decidiu desaplicar a Lei n.º 32/2008 (acórdão n.º 268/2022 do TC de Portugal).

Outra pergunta que se faz: uma entidade administrativa independente pode deliberar no sentido de desaplicar uma lei nas situações submetidas à sua apreciação? Sim, com fulcro no princípio do primado do Direito da União Europeia e da prevalência da Constituição. Mas essa decisão administrativa demonstra a ineficiência de Portugal em relação ao cumprimento do dever de cooperação leal. Onde estavam os poderes Legislativo e Judicial?

Em relação ao reenvio prejudicial, procedimento que não resolve litígios, mas oferece ao juiz nacional elementos para que ele decida conforme a resposta de direito acerca da interpretação ou validade de uma norma da União Europeia, sendo o meio pelo qual o TJUE analisa a interpretação dos Tratados ou a validade e interpretação dos atos das instituições, órgãos ou organismos da União (aqui entre a análise da validade de uma Diretiva). No artigo 267º não há disposição sobre o alcance do acórdão.

Talvez por causa dessa omissão, os pontos do acórdão do TJUE de 08 de abril de 2014, que justificaram a declaração de invalidade da Diretiva 2006/24/CE, não foram automaticamente aplicados em relação à Lei 32/2008 de Portugal, mesmo sendo ela a transposição dessa Diretiva, gerando insegurança jurídica.

A questão da autoridade do acórdão prejudicial é antiga. No livro Contencioso Comunitário, de Maurice-Chistian Bergerés, ele considera que o foco não é sobre a coisa julgada material ou formal, já que em reenvio prejudicial não há litígio e, consequentemente, caso julgado. Segundo esse autor, "*os acórdãos que consideram o acto não válido devem logicamente impor-se a todos os órgãos jurisdicionais nacionais que posteriormente se devam pronunciar.*

A resposta sobre os efeitos do acórdão prejudicial que invalida uma Diretiva pode ser aferida analisando a própria jurisprudência do TJEU.

No acórdão de 13/05/1981, caso *SpA International Chemical Corporation* contra *Amministrazione delle finanze dello Stato* (Identificador ECLI: ECLI:EU:C:1981:102), em um pedido de reenvio prejudicial feito pelo Tribunal Civil de Roma/Itália, processo 66/80, foi decidido que o acórdão do Tribunal que determina a nulidade de um ato de uma instituição da UE, ainda que tenha por destinatário direto apenas o juiz que recorreu ao Tribunal, constitui para qualquer outro juiz motivo suficiente para considerar tal ato inválido para efeitos de decisão que deva proferir:

> *1. La sentenza della Corte che accerti, in forza dell'art. 177 del Trattato CEE, l'invalidità di un atto di un'istituzione, in particolare di un regolamento del Consiglio o della Commissione, sebbene abbia come diretto destinatario solo il giudice che si è rivolto alla Corte, costituisce per qualsiasi altro giudice un motivo sufficiente per considerare tale atto non valido ai fini di una decisione che esso debba emettere; poiché tale constatazione non ha tuttavia l'effetto di privare i giudici nazionali della competenza loro attribuita dall'art. 177 del Trattato, spetta a tali giudici stabilire se vi sia interesse a sollevare nuovamente una questione già risolta dalla Corte nel caso in cui questa abbia constatato in precedenza l'invalidità di un atto di un'istituzione della Comunità. Tale interesse potrebbe, in particolare, esistere qualora sussistessero questioni relative ai motivi, alla portata ed eventualmente alle conseguenze dell'invalidità precedentemente accertata."*

No Processo C-228/92, caso Roquette Frères SA contra Hauptzollamt Geldern (pedido de decisão prejudicial apresentado pelo Finanzgericht Düsseldorf), o TJUE decidiu, no acórdão de 26 de Abril de 1994:

> *2. Se um acórdão do Tribunal de Justiça que declara a título prejudicial a invalidade de um acto comunitário tem, em princípio, efeito retroactivo, da mesma forma que um acórdão de anulação, o Tribunal de Justiça dispõe todavia da faculdade de limitar no tempo os efeitos de uma tal declaração. Essa possibilidade é justificada pela interpretação do artigo 174.° do Tratado, tendo em conta a necessária coerência entre o reenvio prejudicial e o recurso de anulação, que constituem as duas modalidades do controlo da legalidade instituído pelo Tratado. A faculdade de limitar no tempo os efeitos da invalidade de um regulamento comunitário, quer no âmbito do artigo 173.° quer no do artigo 177.°, é uma competência reservada ao Tribunal de Justiça pelo Tratado, no interesse da aplicação uniforme do direito comunitário em toda a Comunidade.*

Segundo DUARTE, Maria Luísa, 2021, p. 384, os efeitos do acórdão da análise de um reenvio prejudicial que declara a invalidade de um ato são:

> "acto declarado inválido é inaplicável no caso concreto e deve ser, nos termos do artigo 266.° TFUE (aplicado por analogia), conjugado com o princípio da cooperação leal, revogado ou alterado, pela instituição, órgão ou organismo que o adoptou; eficácia *ex tunc* é susceptível, por decisão do TJ, de limitação no tempo por razões de interesse relevante."

Conclui-se que a jurisprudência do TJ foi construída equiparando os efeitos do pedido de apreciação de validade com os do recurso de anulação, possibilitando ao Tribunal modular os efeitos da decisão por razões de interesse relevante.

Todavia, quando da análise das questões prejudiciais sobre a validade da Diretiva 2006/24/CE, o TJUE se limitou a declarar sua invalidade. Portanto, no silêncio,

essa decisão deveria ter sido observada pelos países membros, com a invalidação automática das normas internas contrárias aos entendimento do TJUE, providência que não foi tomada por Portugal. Talvez por isso foi tomada a decisão de desaplicação pela Comissão Nacional de Proteção de Dados.

3.2 – Acórdão n.º 268/2022 - declaração de inconstitucionalidade de dispositivos daLei 32/2008

Como acima explanado, o Tribunal Constitucional de Portugal considerou que a Lei 32/2008 não era "uma ação inteiramente determinada pelo Direito da União" (Acórdão 268/2022, nº 20). Por isso, somente anos depois do acórdão do TJUE, o Tribunal Constituicional de Portugal declarou, com força obrigatória geral, a inconstitucionalidade dos artigos 4º , 6º e parcialmente do artigo 9º da Lei 32/2008.

O artigo 4º da Lei 32/2008 previa o armazenamento dos metadados, sem fazer qualquer distinção, abrangendo todas as informações extraíveis dos dados de qualquer forma de comunicação eletrônica. Assim, abrangia as duas categorias de metadados (dados de base e dados de tráfego), sem distingui-los, o que era um erro, pois a tutela constitucional dos metadados das comunicações (dados que não abrangem o conteúdo das comunicações, mas dizem respeito somente às suas circunstâncias) é distinta para as duas espécies.

Dados de base são relativos à identificação dos sujeitos que se conectam à rede, e dados de tráfego são os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência).

Deste modo, a violação aos números 1 e 4 do artigo 35º da CRP só pode ser em relação aos dados de tráfego quando pressuponham uma comunicação entre pessoas (direito à autodeterminação informativa). As outras categorias de metadados (dados de base e dados de tráfego que não pressupõem uma comunicação interpessoal) se submetem a outras garantias constitucionais — designadamente, os direitos à reserva da intimidade da vida privada e ao livre desenvolvimento da personalidade (n.º 1 do artigo 26.º da Constituição).

O artigo 6º previa o armazenamento indiscriminado desses dados por 01 ano. Ou seja, todos os cidadãos ficavam na iminência de terem os seus dados acessados, por 01 ano, mas apenas um rol taxativo de infrações penais poderia ensejar a transmissão de dados, quando fosse imprescindível para a investigação, seguindo

um protocolo rigoroso de segurança para essa transmissão e posterior destruição dos dados comunicados às autoridades públicas. Em suma, o legislador combinou uma obrigação generalizada de os operadores de telecomunicações conservarem todos os dados de base, tráfego e localização (sem delimitar as categorias de dados ou os sujeitos afetados) com um regime vinculado quanto ao respetivo acesso pelas autoridades de investigação criminal.

Já o artigo 9.º da Lei 32/2008 não previa uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal.[334]

Por se tratar de uma ação declaratória de inconstitucionalidade, a justificativa do pedido foi que os artigos 4º e 6º da Lei 32/2008 violavam os números 1 e 4 do artigo 35.º (autodeterminação informativa) e do n.º 1 do artigo 26.º (direito à reserva da intimidade da vida privada), em conjugação com o n.º 2 do artigo n.º 18.º (princípio da proporcionalidade), todos da Constituição das República Portuguesa.[335]

---

[334] Artigo 20.º

Acesso ao direito e tutela jurisdicional efetiva

1. A todos é assegurado o acesso ao direito e aos tribunais para defesa dos seus direitos e interesses legalmente protegidos, não podendo a justiça ser denegada por insuficiência de meios económicos.

[335] Artigo 35.º

Utilização da informática

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

Artigo 26.º

Outros direitos pessoais

1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação.

Artigo 18.º

Força jurídica

2. A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.

O Tribunal Constitucional, no acórdão n.º 268/2022, considerou que a lesão ao n.º 1 do artigo 26.º da CRP ocorreu porque a liberdade de ação é inerente ao desenvolvimento da personalidade e uma das facetas dessa liberdade de ação é a liberdade de se comunicar. Assim, *o direito à reserva da intimidade da vida tutela os indivíduos contra o acesso a um conjunto de informações que dizem respeito apenas aos próprios (por onde circulam, em que momento, em que contextos), envolvendo a proteção constitucional dos dados que permitem retirar conclusões sobre essas circunstâncias.*[336]

Em relação ao artigo 35º da CRP, citando Catarina Sarmento e Castro, o TC considerou que nesse contexto se deve reconhecer *«um direito fundamental à autodeterminação informativa, traduzido num conjunto de direitos relacionados com o tratamento automático das informações pessoais dos cidadãos, que visam, simultaneamente, protegê-las perante ameaças de recolha e de divulgação, assim como de outras utilizações possibilitadas pelas novas tecnologias, e, também, assegurar aos respetivos titulares um conjunto de poderes de escolha nesse âmbito».* Nesse sentido, considerou que o direito à autodeterminação informática tem um âmbito mais amplo do que o direito-garantia à reserva da intimidade da vida privada, sendo um direito defensivo.

Devido a isso, a Constituição atribuiu ao legislador a função de prever garantias de efetividade, impondo medidas de proteção dos dados contra perda, destruição e acesso de terceiros, mas para essas garantias surtirem efeito, os dados têm que estar armazenados em local sob a jurisdição da União Europeia, onde vigoram os padrões de proteção e controlo previstos na CDFUE, no RGPD e nas Constituições dos Estados-membros e nas Leis de transposição das Diretivas correspondentes. Essa conclusão decorre da interpretação do artigo 35.º da CRP, em conformidade com os artigos 7.º e 8.º da CDFUE.

Contudo, como o legislador não determinou que o armazenamento dos dados ocorresse no território da União Europeia, colocou em causa a efetividade dos direitos avalizados pelos n.ºs 1 e 4 do artigo 35.º da Constituição, interpretados em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE. Ademais, mesmo que o legislador tivesse previsto tal obrigação, o armazenamento dos dados de tráfego, de todas as pessoas, sem distinção, por 01 ano, configura uma restrição

336 https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

desproporcionada aos direitos consagrados nos n.ºs 1 e 4 do artigo 35.º e da Constituição, em conjugação com o n.º 1 do artigo 26.º, interpretados em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE.

Em relação aos dados de base (e de endereços de protocolo IP dinâmicos relativos à *fonte* de uma comunicação, independentemente da respetiva categorização), a norma não seria *em si mesma* inconstitucional, se o legislador houvesse cumprido a injunção de prever o seu armazenamento no território da União Europeia. O acórdão sob análise considerou que o armazenamento pelo prazo de 01 ano não era desproporcional para atingir a finalidade de Lei (investigação de crimes graves), até porque esse tipo de investigação é complexa e demorada, não havendo meio menos lesivo com eficácia equivalente.

Contudo, há desproporcionalidade entre o fim almejado e a agressão aos direitos fundamentais à reserva da vida privada e à autodeterminação informativa, o facto da lei atingir todos, inclusivamente os sujeitos relativamente aos quais não há qualquer suspeita de atividade criminosa.

Por fim, o artigo 9º da Lei foi considerado parcialmente inconstitucional por ausência de previsão de notificação aos sujeitos visados de que os dados relativos às suas comunicações foram transmitidos às autoridades públicas (desde que essa comunicação não seja suscetível de comprometer as investigações criminais). Essa é uma, das três condições enunciadas na Diretiva n.º 2002/52/CE para haver conformidade entre o regime de acesso aos dados pelas autoridades públicas e os direitos garantidos pela CDFUE. As outras condições são: limitação ao estritamente necessário para a prevenção, investigação, deteção e repressão de criminalidade grave e controlo judicial ou de entidade administrativa independente.

Por esses fundamentos, assim foi a decisão do TC no acórdão 268/2022:

> *Pelos fundamentos expostos, o Tribunal Constitucional decide:*
> *a) Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição;*
> *b) Declarar a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja*

> *suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.*

Ressalta-se que essa decisão do Tribunal Constitucional causou polêmica entre as autoridades internas. O Sindicato dos Magistrados do Ministério Público (SMMP) entendeu que a decisão do TC iria impossibilitar a investigação criminal, nomeadamente no que diz respeito aos crimes informáticos, acusando ainda o TC de desproteger as vítimas destes crimes (https://www.noticiasdecoimbra.pt/magistrados-dizem-que-decisao-sobre-metadados-impossibilita-investigacao-e-desprotege-vitimas/ acesso em 20/01/2023).

O descontentamento das autoridades portuguesas ensejou outro processo perante o Tribunal Constitucional, numa tentativa frustrada de invalidar esse Acórdão.

Num processo de fiscalização abstrata sucessiva da constitucionalidade a Procuradora-Geral da República arguiu a nulidade do Acórdão n.º 268/2022, com os seguintes fundamentos:

> *— o Ministério Público é defensor da legalidade democrática e interessado na promoção da defesa dos valores constitucionais do Estado de direito democrático e da boa administração e o Acórdão do Tribunal Constitucional n.º 268/2022 «pode vulnerar tais interesses constitucionalmente protegidos»;*
> *— verifica-se contradição entre a fundamentação e a decisão, uma vez que o ponto 18. da fundamentação do Acórdão n.º 268/2022 exclui do juízo de inconstitucionalidade os dados de base, embora o dispositivo declare a inconstitucionalidade de todo o artigo 4.º da Lei n.º 32/2008, de 17 de julho;*
> *— existe omissão de pronúncia, pois «não fixou o Tribunal, expressamente, os efeitos da inconstitucionalidade, permitindo a aplicação retrospectiva, e mesmo retroactiva, da sua doutrina, pondo em risco aqueles interesses constitucionalmente protegidos».*

Contudo, o Tribunal Constitucional, sob a alegação de que não havia previsão legal de incidente pós-decisório relativo a acórdão proferido pelo Tribunal Constitucional em sede de fiscalização abstrata da constitucionalidade e que o processo de fiscalização abstrata sucessiva deveriam ter como sujeitos processuais os mesmos que atuaram no processo originário (a Provedora de Justiça é que era parte na ação original), não conheceu o requerimento, declarando a ilegitimidade

processual e constitucional da Procuradora-Geral da República (Acórdão n.º 382/2022 do Tribunal Constitucional).

Portugal, então, precisava alterar a Lei 32/2008, a fim de regular o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal.

3.3 – Alteração da lei 32/2008 – Acórdão nº. 800/2023

Em 26 de outubro de 2023 foi publicado, no Diário da Assembleia da República, o Decreto n.º 91/XV da Assembleia da República tendo como objeto a segunda alteração à Lei n.º 32/2008 (lei de transposição, para a ordem jurídica interna, da Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março), relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, a fim de conformá-la com o Acórdão do Tribunal Constitucional n.º 268/2022.

Essas foram as alterações dos artigos 4º, 6º e 9º:

> *Artigo 4.º*
> *1 – Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar, nos termos previstos na presente lei, em Portugal ou no território de outro Estado-Membro da União Europeia, as seguintes categorias de dados:*
>
> *Artigo 6.º*
> *Período e regras de conservação*
> *1 – Para efeitos da finalidade prevista no n.º 1 do artigo 3.º, as entidades referidas no n.º 1 do artigo 4.º devem conservar, pelo período de um ano a contar da data da conclusão da comunicação, os seguintes dados:*
> *a) Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações;*
> *b) Os demais dados de base;*
> *c) Os endereços de protocolo IP atribuídos à fonte de uma ligação.*
> *2 – Os dados de tráfego e de localização são conservados pelas entidades referidas no n.º 1 do artigo 4.º pelo período de três meses a contar da data da conclusão da comunicação, considerando-se esse período prorrogado até seis meses, salvo se o seu titular se tiver oposto perante as referidas entidades à prorrogação dessa conservação.*
> *3 – Os prazos de conservação previstos no número anterior podem ser prorrogados por períodos de três meses até ao limite máximo de um ano, mediante autorização judicial, requerida pelo Procurador-Geral*

da República, fundada na sua necessidade para a finalidade prevista no n.º 1 do artigo 3.º.
4 – A prorrogação do prazo de conservação referida nos números anteriores deve limitar-se ao estritamente necessário para a prossecução da finalidade prevista no n.º 1 do artigo 3.º, devendo cessar logo que se confirme a desnecessidade da sua conservação.
5 – As entidades referidas no n.º 1 do artigo 4.º não podem aceder aos dados aí elencados salvo nos casos previstos na lei ou definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais.
6 – A autorização judicial a que se refere o n.º 3 compete a uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções.

Artigo 9.º
2 – A autorização prevista no número anterior só pode ser requerida pelo Ministério Público.
7 – Sem prejuízo do disposto no número seguinte, o despacho que autoriza a transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º é notificado ao titular dos dados no prazo máximo de 10 dias a contar da sua prolação.
8 – Se, em inquérito, o Ministério Público considerar que a notificação referida no número anterior comporta risco de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas, pode solicitar ao juiz de instrução criminal que protele a notificação, a qual é realizada logo que a razão do protelamento deixar de existir ou, o mais tardar, no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento desta fase processual.
9 – A transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º a autoridades de outros Estados só pode ocorrer no âmbito da cooperação judiciária internacional em matéria penal, de acordo com as regras fixadas na respetiva lei e desde que esses Estados garantam o mesmo nível de proteção de dados pessoais vigente no território da União Europeia.

Observa-se que há distinção entre dados de tráfego e dados de base, podendo, aqueles, serem armazenados por 03 meses e estes, por 01 ano. Também há previsão de que o armazenamento ocorra dentro da União Europeia, bem como que o titular dos dados que foram acessados/transmitidos às autoridades sejam notificados.

Contudo, ainda restavam dúvidas se essas alterações da Lei 32/2008 eram suficiente para resguardar o direito à privacidade e a autodeterminação informacional, no contexto da proteção de dados da Constituição da República Portuguesa, a jurisprudência afirmada no Acórdão n.º 268/2022 e o regime aplicável de Direito Europeu, razão pela qual o Presidente da República, quando recebeu o

Decreto para promulgação como Lei, com fulcro no n.º 1 do artigo 278.º da Constituição da República Portuguesa, requereu ao Tribunal Constitucional a apreciação preventiva de sua constitucionalidade.

No acórdão foi destacado os seguintes pontos:

1) a previsão de armazenamento de dados no território da União Europeia sanou a omissão existente na redação anterior e é constitucional, por viabilizar os mecanismos de garantia e controlo das normas vigentes na UE.
2) Inovação no sentido de diferençar os metadados em categorias de dados para dar proteção diferenciada. Nesse ponto, foi analisado o princípio da proporcionalidade, já que estavam em causa direitos fundamentais: de um lado, o combate à criminalidade e, do outro, as ingerências aos direitos à reserva a privacidade e à autodeterminação informacional, afetados pela conservação dos dados, mesmo sendo essa medida necessária para efetivar os objetivos da Lei, que foram considerados legítimos. No mesmo sentido do acórdão 268/2022, a conservação dos dados de base por um período de 01 ano não foi considerada em si mesma inconstitucional. Em relação a alteração do prazo de conservação dos dados de tráfego (3 meses, prorrogáveis por até 6 meses se não tiver oposição do titular), o TC considerou que, por traçarem um perfil pormenorizado do titular, principalmente por conterem dados de localização, a ingerência tinha que ser menor e mais especificada, sob pena de colocar em risco desproporcional a vida privada do titular. Nesse sentido, por não mencionar prazos específicos de conservação de dados de tráfico e de localização; por não dirigir, de forma direta, objetiva e não discriminatória, apenas às pessoas relacionadas à investigação criminal, e por permitir, de forma subjetiva, a prorrogação do prazo, não chegou ao patamar da consitucionalidade.
3) Em relação a inconstitucionalidade do artigo 9º, esta restou sanada pelo facto do Decreto prever a notificação do titular dos dados acessados/transferidos para a autoridade.

Assim foi a decisão desse acórdão:

> *Pelos fundamentos expostos, o Tribunal Constitucional decide:*
> *(a) Pronunciar-se pela inconstitucionalidade da norma constante do artigo 2.º do Decreto n.º 91/XV, da Assembleia da República, publicado no Diário da Assembleia da República n.º 26, II Série A, de 26 de outubro de 2023, e enviado ao Presidente da República para*

promulgação como lei, na parte em que altera o artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugado com o artigo 6.º da mesma lei, quanto aos dados previstos no n.º 2 do mencionado artigo 6.º, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição;
(b) Não se pronunciar pela inconstitucionalidade das demais normas cuja apreciação foi requerida.

Vale ressaltar que houve 3 votos vencidos.

Sem desconsiderar a vasta jurisprudência do TJUE, que serviu de parâmetro para este acórdão e para o acórdão 268/2022, nos votos vencidos foram destacados que Estados-membros vêm reagindo à tendência do TJUE de, em alguns casos, conferir um alcance muito amplo aos direitos ao respeito pela vida privada e à proteção dos dados pessoais, em detrimento da proteção devida a outros direitos fundamentais como a segurança, que é base para dignidade social de todos os cidadãos.

Ademais, essa exacerbada proteção está por invadir prerrogativas exclusivas dos Estados-Membros em matéria de segurança pública e de prevenção, investigação, deteção e repressão de infrações penais, sendo, os dados de tráfego e de localização, um elemento imprescindível para a investigação, deteção e repressão de crimes graves, sendo, em muitos casos, a única forma de encontrar os autores das infrações. Contudo, o armazenamento seletivo de dados acaba por inviabilizar esse meio de investigação.

A magistrada Joana Fernandes Costa considerou que o legislador de 2023 procurou, através das alterações constantes do Decreto sob apreciação, preencher o vazio normativo que resultou da declaração com força obrigatória geral resultante do Acórdão n.º 268/2022, e que a preservação dos dados de tráfego e de localização com vista à prevenção, investigação, deteção e repressão da criminalidade grave só será eficaz, e até mesmo legítima, se o acesso for exequível seja quem for a pessoa sobre quem vier a recair a suspeita da atividade ilícita, desiderato que não é propiciado pela conservação seletiva daquele tipo de metadados.

Todavia, aduz que o TJUE, ao elevar a tão alto patamar a tutela dos direitos ao respeito pela reserva da vida privada, à proteção dos dados pessoais e à liberdade de expressão, pôs em cheque a proteção dos direitos fundamentais das

pessoas afetadas por crimes graves, configurando uma falta de solidariedade para com os membros comunitários.

Observa a difícil aplicação do princípio da proporcinalidade, previsto no artigo 52º, n. 1, da própria Carta do Direitos Fundamentais da União Europeia.

Conclusão

Quando se fala em armazenamento de metadados, há a necessidade de aferir a validade de uma lei com base nos parâmetros constitucionais, que, por sua vez, têm que convergir com o direito da União Europeia. Nesse contexto, deve ainda ter em conta a disciplina do Regulamento Geral sobre a Proteção de Dados (Regulamento UE 2016/679 — RGPD), que vincula todos os sujeitos públicos e privados, em toda a União — artigo 288.º TFUE. Por isso, o tratamento de dados pessoais operado pelos fornecedores de comunicações eletrónicas em Portugal tem que respeitar as regras do RGPD (artigo 3.º do RGPD).

Com efeito, os dados de base, de tráfego e de localização, na medida em que permitam identificar uma pessoa singular (n.º 1 do artigo 4.º do RGPD), deve ser tratados, e esse tratamento segue alguns princípios. Segundo Francisca Cardoso Resende Gomes, *a operatividade de todo este feixe de direitos faz-se com a orientação de certos princípios que têm vindo a ser elencados pela doutrina e operacionalizados pela jurisprudência constitucional e europeia, com destaque para os princípios da transparência, da especificação das finalidades, da fidelidade e de limitação da utilização.os princípios da transparência, da especificação das finalidades, da fidelidade e de limitação da utilização*.

Os dados só podem ser recolhidos para satisfazer finalidades determinadas, explícitas e legítimas, e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades (alínea b) do n.º 1 do artigo 5.º do RGDP) e a sua conservação só pode ocorrer durante o período necessário para as finalidades para as quais são tratados (alínea e) do n.º 1 do artigo 5.º do RGDP).

Esses princípios decorrem dos direitos fundamentais à vida privada e à autodeterminação informacional, que foram o fundamento dos acórdãos analisados no presente trabalho.

O direito à proteção de dados consiste em um direito fundamental com dimensão positiva e negativa. Por estar no rol dos direitos, liberdades e garantias, tem caráter defensivo ao tutelar a reserva sobre factos cujo conhecimento por terceiros deve depender do consentimento do seu titular, não podendo haver ingerência do Estado relativamente a dados informativos que pertencem ao cidadão (carater negativo).

Apesar da dignidade constitucional que lhe é atribuída, a proteção de dados exige a intervenção do legislador, devendo, a norma regulamentadora desse direito, conferir a máxima efetivação da autodeterminação da pessoa sobre os seus dados. Por isso as restrições ou limitações a esse direito, mesmo que previstas em Lei, devem ser analisadas com muita cautela, sob pena constituir inconstitucionalidade.

Nos termos do artigo 52.º da Carta, restrições a direitos fundamentais só podem ser feitas por lei se forem necessárias e nos limites dos objetivos de interesse geral a alcançar. Assim deve ser aplicado o princípio da proporcionalidade.

Um Estado-Membro pode adotar legislação que permita a conservação dos metadados, para efeitos de luta contra a criminalidade grave, mas essas normas têm de ser claras e precisas, com exigências mínimas, de modo que as pessoas cujos dados foram conservados possam se proteger contra os riscos de abuso, e desde que a conservação dos dados seja limitada ao estritamente necessário, dentro do objetivo prosseguido.

Teoricamente, aplicar o princípio da proporcionalidade nesse caso é fácil, mas algumas situações práticas são difíceis de resolver. Se, para preservar a privacidade das pessoas a lei condiciona o armazenado à vinculação da pessoa com a prática de uma infração penal grave, acaba por obstar a descoberta de autores de crimes se, na época de se determinar o armazenamento, aquela pessoa ainda não era suspeita, mas depois, passou a ser e seus dados não foram armazenados.

Por sua vez, se o prazo do armazenamento é muito curto, pode ocorrer que, quando a investigação atingir o patamar de se acessar esses dados, eles já não existam.

É certo que nenhum direito fundamental, por mais relevante que seja, é absoluto e, nessas situações de conflito a ponderação é imprescindível. Limitar o conteúdo de um direito, em determinadas situações e sob determinados pressupostos, pode ser necessáario para atingir um bem maior.

Por isso, as alterações que vierem a ser feitas na Lei 32/2008 tem que achar esse ponto de equilíbrio, como, por exemplo, determinar a encriptação dos dados a serem transmitidos para as autoridades e limitar o acesso a esses dados, através de mecanismos de segurança rígidos.

Referências bibliográficas

BERGERÈS, Maurice-Christian, Contencioso Comunitário, Tradução de Evaristo Santos, Colecção Resjurídica.

COMPARATO, Fábio Konder. Afirmação Histórica dos Direitos Humanos. São Paulo: Saraiva, 2003. ISBN 85-02-04077-4

CRORIE, Benedita Mac, O Recurso ao Princípio da Dignidade da Pessoa Humana na Jurisprudência do Tribunal Constitucional – Estudos em Comemoração do Décimo Aniversário da Licenciatura em Direito da Universidade do Minho, Almedina, 2003.
Warren e Brandeis, Direito à Privacidade, Harvard Law Review, Vol. IV 15 de dezembro de 1890 nº 5 pdf https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

DUARTE, Maria Luísa, Direito da União Europeia – lições desenvolvidas. AAFDL Editora, 2021.

RODOTÀ, Stefano. Data protection as a fundamental right. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; TERWANGNE, Cécile de; NOUWT, Sjaak. (ed.). Reinventing data protection?. Dordrecht: Springer, 2009. cap. 3, p. 77-82. Disponível em: https://doi.org/10.1007/978-1-4020-9498-9_3.

WARREN, Samuel D.; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: http://www.jstor.org/stable/1321160.

Jurisprudência:

TRUBUNAL DE JUSTIÇA DA UNIIÃO EUROPEIA

- Acórdão do Tribunal de 13 de Maio de 1981, SpA International Chemical Corporation v Amministrazione delle finanze dello Stato, Pedido de decisão prejudicial: Tribunale civile e penale di Roma – Itália, Caso 66/80, acesso em 19/01/2023 – pdf https://curia.europa.eu/juris/fiche.jsf?id=C;66;80;RP;1;P;1;C1980/0066/J&language=en

- Acórdão do Tribunal de Justiça de 26 de Abril de 1994, Processo C-228/92, Roquette Frères SA contra Hauptzollamt Geldern (pedido de decisão

prejudicial apresentado pelo Finanzgericht Düsseldorf) – acesso em 19/01/2023, pdf https://curia.europa.eu/juris/showPdf.jsf?docid=98592&doclang=PT

- Acordão de 08 de abril de 2014

TRIBUNAL CONSTITUCIONAL DE PORTUGAL

- Acódão 286/2022 de 03 de junho, pdf 500 Internal Server Error (tribunalconstitucional.pt)

- Acódão 382, pdf 500 Internal Server Error (tribunalconstitucional.pt)

- Acórdão 800/2023, pdf https://www.tribunalconstitucional.pt/tc/acordaos/20230800.html

Normas

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, Deliberação n.º 1008/2017, https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2017&type=2&ent=

DIÁRIO DA REPÚBLICA. Decreto de 10 de Abril de 1976 - Constituição da República Portuguesa, Diário de República n.º 86/1976, Série I de 1976-04-10, páginas 738 – 775, Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-aprovacao-constituicao/1976-502635

DIÁRIO DA REÚBLICA, I Série, n.º 57/78, de 9 de Março de 1978 - Declaração Universal dos Direitos Humanos

DIÁRIO DA REPÚBLICA I-A, n.º 159, de 09/07/1993 (Resolução da Assembleia da República n.º 23/93) - Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/107-2023-221100280

DIÁRIO DA REPÚBLICA n.º 137/2008, Série I de 2008-07-17, páginas 4454 – 4458 – Lei 32/2008, de 17 de julho, Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. Disponível em https://diariodarepublica.pt/dr/detalhe/lei/32-2008-456812

DIÁRIO DA REPÚBLICA n.º 169/2023, Série I de 2023-08-31, páginas 83 – 112 - Resolução da Assembleia da Republica n.º 107/2023, de 31 de Agosto. Aprova o Protocolo que Altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal

DIÁRIO DE REPÚBLICA n.º 44, Série II de 07 de dezembro de 2023 DECRETO DA ASSEMBLEIA DA REPÚBLICA N.º 91/XV

JORNAL OFICIAL DA UNIÃO EUROPEIA nº L 281 de 23/11/1995 p. 0031 – 0050 - Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

JORNAL OFICIAL DA UNIÃO EUROPEIA DIRECTIVA 2006/24/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de Março de 2006 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024

JORNAL OFICIAL DA UNIÃO EUROPEIA de 7.6.2016, C 202/289 - Carta dos Direitos Fundamentais da União Europeia

JORNAL OFICIAL DA UNIÃO EUROPEIA - L 119/89 de 4.5.2016 - DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, 04 de maio de 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680

TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM – Conselho da Europa - Convenção Europeia dos Direitos Humanos de 02/04/2013.

Links
https://www.noticiasdecoimbra.pt/magistrados-dizem-que-decisao-sobre-metadados-impossibilita-investigacao-e-desprotege-vitimas/

A Legalidade do Acesso a Registos, Dados Cadastrais, Documentos e Informações em Sede de Investigações Criminais

Joana Maria de Oliveira Moreira[337]

Resumo

O acesso a registos, dados cadastrais, documentos e informações depende de uma série de fatores, tais como o objetivo da investigação, o tipo de informação solicitada e a privacidade das pessoas envolvidas. Efetivamente o Ministério Público e, por conseguinte, os órgãos de polícia criminal, têm a possibilidade de aceder a registos, dados e documentos de terceiros para fins de investigação. No entanto, o acesso está limitado pela proteção do direito à intimidade da vida privada, protegido pela Lei Fundamental no seu artigo 26.º. Outras entidades como as Conservatórias ou o Serviço de Estrangeiros e Fronteiras podem por exemplo, aceder ao registo criminal dos cidadãos que visem alterar o seu nome ou nos processos de nacionalidade, no primeiro caso e no segundo caso, para adquirir um visto de residência. É importante que os procedimentos de recolha de informações sejam regulados por lei e que as pessoas singulares e coletivas, alvos de investigações, sejam notificadas sobre o acesso às suas informações. Além disso, as autoridades devem seguir as diretrizes estabelecidas pelas leis de proteção de dados pessoais, garantindo que as informações recolhidas sejam usadas de maneira apropriada e que sejam protegidos os direitos dos indivíduos. Por conseguinte, este artigo fará um passeio pelo ordenamento brasileiro bem como, pelo português para perceber em que "pé" se encontram os mesmos, relativamente a tal temática. Recorrer-se-á igualmente ao Direito da União Europeia para entendermos qual a sua visão.

Palavras-chave: Dados Pessoais, Confidencialidade, Investigação, Legislação.

[337] Joana Moreira, Assistente Convidada da Unidade Curricular de Direito Processual Administrativo na Universidade Europeia desde 2022. Licenciada em Direito (2022) e Mestranda em Direito Judiciário pela mesma instituição.

A Legalidade do Acesso a Registos, Dados Cadastrais, Documentos e Informações em Sede de Investigações Criminais

Joana Maria de Oliveira Moreira

Abstract
Access to records, registration data, documents and information depends on a number of factors, such as the purpose of the investigation, the type of information requested, and the privacy of the persons involved. Indeed, the Public Prosecutor's Office and, therefore, the criminal police bodies, have the possibility of accessing third party records, data and documents for research purposes. However, access is limited by the protection of the right to privacy of private life, protected by the Fundamental Law in Article 26. Other entities such as the Conservatoires or the Foreigners and Borders Office may, for example, access the criminal record of citizens who aim to change their name or in nationality proceedings, in the first case and in the second case, to acquire a residence visa. Is important that the procedures for collecting information are regulated by law and that natural and legal persons who are the subject of investigations are notified of access to their information. In addition, authorities must follow the guidelines established by personal data protection laws, ensuring that the information collected is used appropriately and that the rights of individuals are protected. Therefore, this report will take a tour of the Brazilian order as well as, by the Portuguese to understand in what place they are in, in relation to this theme. European Union law will also be used to understand what its vision is.

Key words: Personal Data, Confidentiality, Investigation, Legislation.

Introdução

O direito à reserva sobre a intimidade privada é um direito basilar do nosso sistema ao ponto que detém consagração constitucional no artigo 26.º da Constituição da República Portuguesa (CRP). Aliás, esse mesmo expõe que "A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias" (artigo 26.º, n.º 2 da CRP).

Inclusive a Declaração Universal dos Direitos Humanos (DUDH) no seu artigo 12.º estabelece que: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

No mesmo sentido, dispõe o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP) no seu artigo 17.º, n.º 1 que "Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação".

No entanto, por vezes essas ingerências na vida privada são necessárias para a prossecução de valores como a segurança pública. A própria Convenção Europeia dos Direitos Humanos (CEDH) estabelece isso quando no seu artigo 8.º, n.º 2 sublinha que "Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiro".

Face a isso, o ordenamento jurídico brasileiro detém todo um regime quanto à matéria do "Acesso a Registos, Dados Cadastrais, Documentos e Informações". O mesmo consta da Lei n.º 12.850/13, de 2 de agosto de 2013 que tem como escopo: "Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências".

Começando este diploma por tratar das organizações criminosas, é preciso saber no que estas consistem. A Convenção das Nações Unidas Contra a Criminalidade Organizada Transnacional[338], também conhecida como Convenção de Palermo, define no seu artigo 2.º, alínea a), «Grupo criminoso organizado» como "um grupo estruturado de três ou mais pessoas, existindo durante um período de tempo e atuando concertadamente com a finalidade de cometer um ou mais crimes graves ou infrações (…), com a intenção de obter, direta ou indiretamente, um benefício económico ou outro benefício material".

A criminalidade organizada é uma ameaça séria à segurança e estabilidade de uma sociedade, pois esses grupos criminosos têm recursos financeiros e operacionais significativos podendo por isso afetar negativamente a economia e a política de um país. Além disso, a criminalidade organizada pode intimidar ou ameaçar a população, corromper instituições públicas e privadas, e prejudicar o desenvolvimento social e económico de uma região.

Para combater a criminalidade organizada, é necessário um esforço internacional coordenado, que envolva a cooperação entre países, agências de aplicação da lei e organizações internacionais. Isso inclui a intensificação das investigações, o aumento da capacidade de processar e julgar os suspeitos, e o fortalecimento da legislação e dos sistemas judiciários para lidar com a criminalidade organizada.

Além disso, é importante abordar as causas subjacentes à criminalidade organizada, tais como a pobreza, a desigualdade e a falta de oportunidades econômicas, para evitar que as pessoas sejam atraídas para esse estilo de vida.

"As origens das organizações criminosas em nosso mundo podem nos remeter a vários países tais como Itália, com a Máfia Italiana, o qual diversas "famílias" tais como a "Cosa Nostra" se organizavam para realizar práticas ilícitas tais como contrabando de mercadorias, extorsão, tráfico de drogas, lavagem de dinheiro, bem como financiamento de campanhas eleitorais, para que tivesse influência na política daquele país. Outra organização bastante conhecida é a "Yakusa" do

338 Diário da República I-A, n.º 79, de 02/04/2004 (Resolução da Assembleia da República n.º 32/2004).

Japão, dominando as práticas ilícitas de tráfico de drogas e de pessoas, prostituição, pornografia e extorsão"[339].

O artigo 288.º do Código Penal brasileiro, transposto no Decreto-Lei nº 2.848, de 07 de Dezembro de 1940 tem como epígrafe "Associação Criminosa" dizendo-nos que: Associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes: Pena – reclusão, de 1 (um) a 3 (três) anos. Parágrafo único. A pena aumenta-se até a metade se a associação é armada ou se houver a participação de criança ou adolescente".

O artigo 1.º, §1.º da Lei n.º 12.850/13, diz-nos que "Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional".

Já na legislação portuguesa, o artigo 299.º, n.º 1 do Código Penal (CP) entende como "Associação criminosa": "Quem promover ou fundar grupo, organização ou associação, cuja, finalidade ou atividade seja, dirigida à prática de um ou mais crimes, é punido com pena de prisão de um a cinco anos". Nos termos do n.º 2 desse mesmo artigo "Na mesma pena incorre quem fizer parte de tais grupos, organizações ou associações ou quem os apoiar, nomeadamente fornecendo armas, munições, instrumentos de crime, guarda ou locais para as reuniões, ou qualquer auxílio para que se recrutem novos elementos". O n.º 3 desse disposto indica que "Quem chefiar ou dirigir os grupos, organizações ou associações referidas nos números anteriores é punido com pena de prisão de dois a oito anos". Quanto ao seu n.º 5 "(…) considera-se que existe grupo, organização ou associação quando esteja em causa um conjunto de, pelo menos, três pessoas, atuando concertadamente durante um certo período de tempo".

O crime de associação criminosa apresenta-se como um crime formal, ou seja, é um crime em que a ofensa do bem jurídico não depende da lesão de qualquer objeto material da ação; basta-se com a conduta. No caso em concreto, o crime de associação criminosa consome-se pela mera associação de pessoas,

[339] Jusbrasil – "Organização Criminosa - Lei 12.850/13 – Ação Controlada, Infiltração de Agentes e Acesso a Registros".

independentemente da execução dos crimes que planeiam e que originaram esta associação.

"Para que configure uma organização criminosa é necessário que haja uma divisão de tarefas entres os integrantes, porém todos serão autores da conduta tipificada, independente do seu grau hierárquico na estrutura. Assim, conclui-se que todos serão coautores; o líder da organização terá um agravante em sua conduta, pois exerce a liderança, mesmo que não execute atos criminosos"[340].

1. O Acesso a Registos, Dados Cadastrais, Documentos e Informações Enquanto Meio de Obtenção de Prova: Portugal vs. Brasil

Nos termos da lei portuguesa, o Código de Processo Penal (CPP) dispõe de um capítulo próprio quanto a este meio de obtenção de prova. Desse retiramos que "Constituem objeto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis", é isto que nos diz o artigo 124.º, n.º 1. Por sua vez o artigo 125.º estabelece que "São admissíveis as provas que não forem proibidas por lei.". Quanto à prova documental, a mesma consta dos artigos 164.º e seguintes desse mesmo diploma.

No que concerne à Lei Fundamental Portuguesa, a mesma estabelece no artigo 34.º, n.º 2 que "O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis". O n.º 4 desse mesmo artigo, expõe que "É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal".

Quanto a essa matéria, o artigo 252.º-A, n.º 1 do CPP, sublinha que "As autoridades judiciárias e as autoridades de polícia criminal podem obter dados sobre a localização celular quando eles forem necessários para afastar perigo para a vida ou de ofensa à integridade física grave". No entanto, "Se os dados sobre a localização celular previstos no número anterior se referirem a um processo em curso, a sua obtenção deve ser comunicada ao juiz no prazo máximo de quarenta e oito horas" (artigo 252.º-A, n.º 2 do CPP).

340 Jusbrasil – "Organização Criminosa - Lei 12.850/13 – Ação Controlada, Infiltração de Agentes e Acesso a Registros".

Já no caso de não haver nenhuma investigação em curso, "a comunicação deve ser dirigida ao juiz da sede da entidade competente para a investigação criminal" (artigo 252.º-A, n.º 3 do CPP).

Se a obtenção de dados sobre a localização celular não respeitar essas indicações, essa obtenção é nula nos termos do artigo 252.º-A, n.º 4 do CPP.

De notar que, "A interceção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público", é isto que estabelece o artigo 187.º do CPP.

Já quanto à lei brasileira, é possível recorrer aos meios do artigo 3.º da Lei n.º 12.850/13, por forma a obter a prova necessária. Nesse sentido, são permitidas: (I) a colaboração premiada, (II) a captação ambiental de sinais eletromagnéticos, óticos ou acústicos, (III) a ação controlada, (IV) o acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais, (V) intercetação de comunicações telefônicas e telemáticas, nos termos da legislação específica, (VI) afastamento dos sigilos financeiro, bancário e fiscal, (VII) infiltração, por policiais, em atividade de investigação e, (VIII) a cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal.

Em concreto, vamos perceber que o Delegado de Polícia e do Ministério Público podem requisitar o acesso a registos, dados cadastrais, documentos e informações de indivíduos que estejam a ser investigados dentro de uma organização criminosa. Esse acesso permite traçar um perfil mais cuidado os integrantes da organização bem como, descobrir qual a sua atual localização.

A Secção IV da Lei n.º 12.850/13 trata disso mesmo. O artigo 15.º estabelece então que "O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartões de crédito".

Como sabemos, a filiação consiste na indicação do nome do pai e da mãe. A indicação do endereço, consiste na indicação precisa do local de residência e de trabalho, caso ambos os dados estejam disponíveis.

No que concerne às instituições financeiras e administradoras de cartões de crédito, tratando-se de informações sensíveis e, "indubitavelmente, protegidas pelo sigilo bancário, o acesso deve se restringir aos dados cadastrais para a abertura das contas correntes ou aplicações financeiras, bem como para a solicitação dos cartões de crédito. Não estão incluídos no conceito de "dados cadastrais" a data de abertura da conta corrente ou de início de utilização do cartão de crédito, a identificação das contas correntes de origem e de destino de operações financeiras, as datas e valores de tais operações, nem mesmo o volume total de movimentação financeira em um determinado período. Todos estes dados são protegidos pelo sigilo bancário, enquanto forma de resguardar a intimidade e o acesso a eles depende de prévia autorização judicial"[341].

Quanto aos provedores de internet, "novamente não se poderá ter acesso, sem ordem judicial, a dados que extrapolem as simples informações cadastrais. Será possível saber quais os dados cadastrais informados para a abertura de uma conta de email, de um blog, ou dos serviços de acesso do provedor. Por outro lado, estarão protegidos pela intimidade, as senhas de acesso utilizadas, o conteúdo dos emails e informações sobre com quem há trocas de mensagens eletrônicas, as datas e horas de tais mensagens etc. Também não se poderá solicitar informações sobre sites visitados"[342].

Nos termos do artigo 16.º dessa IV Secção: "As empresas de transporte possibilitarão, pelo prazo de 5 (cinco) anos, acesso direto e permanente do juiz, do Ministério Público ou do delegado de polícia aos bancos de dados de reservas e registo de viagens".

Tratando-se de empresas de transportes públicos, não se colocam quaisquer questões de direito à privacidade pois, quem anda de autocarro, metro, comboio ou até mesmo, voa por meio de uma empresa comercial, não está a praticar um ato

[341] BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014), p. 16.

[342] BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014), p. 17.

no âmbito restrito da sua vida privada. "Isto porque o transporte público é de livre acesso a todos e quem opta por utilizá-lo, não poderá esperar qualquer forma de reserva ou sigilo"[343].

"A questão, contudo, será diversa, no caso de empresas de transporte particular. Por exemplo, empresas de táxi-aéreo ou de aluguel de veículos particulares. Nestes casos, é razoável considerar que a utilização do transporte pode envolver aspetos de âmbito privado, como por exemplo, visitar uma pessoa ou ir a um determinado local de forma reservada, sem que isso se torne do conhecimento de todos. Nesse caso, a medida deverá ser precedida de ordem judicial, sob pena de caracterizar indevida restrição da intimidade, gerando a ilicitude da prova obtida"[344].

E o 17.º artigo estabelece que "As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no artigo 15.º, registos de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais".

Apesar do disposto, entende-se necessária a requisição prévia de uma autorização judicial. Se não fosse assim, tal "seria inconstitucional, na medida em que o acesso aos dados relativos às ligações telefônicas nele previsto, como números das linhas de origem e destino da ligação, embora não impliquem intercetação de comunicações telefônicas, podem envolver aspetos da intimidade e da vida privada do usuário do serviço de telefônica"[345].

O prazo de 5 anos que está estatuído, implica que "os dados deverão ser preservados e ficarão "à disposição" das autoridades policiais e do Ministério Público (MP). Estar "à disposição" não é o mesmo que "ter acesso, independentemente de autorização judicial", como prevê, por exemplo, o artigo 15.º. Ou seja, os dados estão

[343] BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014), p. 17.

[344] BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014), págs. 18 e 19.

[345] BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014), p. 18.

à disposição, isto é, disponíveis, mas para a eles se ter acesso, será necessária prévia autorização judicial"[346].

Nos termos do artigo 21.º da Lei n.º 12.850/13 "Recusar ou omitir dados cadastrais, registos, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. Parágrafo único. Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei".

Neste caso concreto, o bem jurídico aqui tutelado é "a boa e regular Administração da Justiça, que, necessariamente, é atingida pelo descumprimento ou desatendimento de diligências determinadas pelas autoridades que a representam, especialmente no curso de investigações criminais, mormente naquelas relativas a crimes graves, como os eventualmente praticados por uma organização criminosa"[347].

O sujeito ativo do ato constante do artigo 21.º pode ser qualquer pessoa, mas de um modo geral, será um funcionário público que não atendeu à requisição que fora efetuada pelas autoridades. O sujeito passivo será obviamente o Estado.

"As condutas descritas no parágrafo único, por sua vez, configuram crimes próprios, isto é, só podem ser praticados pelas autoridades requisitantes e seus assessores que tomam conhecimento dos resultados das diligências realizadas. As demais pessoas, digamos comuns, isto é, não envolvidas oficialmente com a matéria, não têm esse dever legal de fidelidade funcional"[348].

A conduta descrita no artigo 21.º é do tipo dolosa, dolo esse que é "representado pela vontade livre e consciente de recusar ou omitir requisição efetuada pelas autoridades mencionadas, total ou parcialmente. É necessário, inclusive, que o agente tenha consciência do seu dever funcional de atender à

[346] BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014), p. 18.

[347] BITENCOURT, CEZAR ROBERTO – "Sonegação de Informações Requisitadas", R. EMERJ, Rio de Janeiro, v. 18, n. 67 (2015), p. 221.

[348] BITENCOURT, CEZAR ROBERTO – "Sonegação de Informações Requisitadas", R. EMERJ, Rio de Janeiro, v. 18, n. 67 (2015), p. 223.

requisição recebida (…)"[349]. Denoto que, este crime consome-se no momento em que o sujeito passivo recusa ou omite o atendimento da requisição feita.

A atribuição do delegado de polícia está restrita à fase investigatória. Uma vez intentada à ação penal, essa atribuição pertence ao MP. Por estes, podem ser requisitados:

(i) Dados cadastrais, como já mencionado anteriormente, o nome da pessoa alvo da investigação, os seus laços familiares, idade, formação, entre outros;

(ii) Registos, como trabalhos realizados, acontecimentos promovidos por si, acontecimentos nos quais participou, que sejam pertinentes para a investigação;

(iii) Documentos, sendo documento todo o instrumento "que sirva de base material para registar manifestações de vontade"[350];

(iv) Informações, que são todos e quaisquer outros elementos e circunstâncias que devam ser objeto de investigação e que podem interessar à entidade que os requer.

2. A Diretiva (UE) 2016/680 de 27 de abril de 2016

Estando a tecnologia e a forma como se armazenam e protegem dados pessoais sempre em evolução, em sede de Direito da União Europeia (UE), o Parlamento Europeu e o Conselho, publicaram a Diretiva (UE) 2016/680 de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, esta relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

[349] BITENCOURT, CEZAR ROBERTO – "Sonegação de Informações Requisitadas", R. EMERJ, Rio de Janeiro, v. 18, n. 67 (2015), p. 230.

[350] BITENCOURT, CEZAR ROBERTO – "Sonegação de Informações Requisitadas", R. EMERJ, Rio de Janeiro, v. 18, n. 67 (2015), p. 225.

Tal tema precisou de ser tratado cuidadosamente, por estas instituições da União saberem melhor que ninguém que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental, direito fundamental este consagrado tanto no artigo 8.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia (CDFUE) e o artigo 16.º, n.º 1 do Tratado sobre o Funcionamento da União Europeia (TFUE).

Tanto um artigo como outro dispõem que: "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Denoto que as duas instituições mencionadas acima, têm competência para legislar sobre esta matéria nos termos do artigo 16.º, n.º 2 do TFUE.

Além disso e tal como sublinha o 2º considerando da Diretiva "(…) A tecnologia permite o tratamento de dados pessoais numa escala sem precedentes para o exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais e a execução de sanções penais". Inclui-se aí também, a salvaguarda e a prevenção de ameaças à segurança pública.

Quando se transferem dados pessoais com esse intuito, entre autoridades competentes, países terceiros e organizações internacionais, essa transferência deve de ser por um lado facilitada por forma a assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial.

Por outro lado, deve ser assegurado um elevado nível de proteção de dados pessoais por se estes implicarem informações sensíveis quanto à pessoa ou pessoas alvo de investigação.

A Diretiva refere que todos os Estados-Membros fazem parte da Organização Internacional da Polícia Criminal, mais conhecida como Interpol. Esta, "no exercício das suas atribuições (…) recebe, conserva e divulga dados pessoais a fim de auxiliar as autoridades competentes na prevenção e no combate à criminalidade internacional".

Por conseguinte, é conveniente reforçar a cooperação entre a União e a Interpol mediante a promoção de um eficaz intercâmbio de dados pessoais, assegurando ao mesmo tempo o respeito pelos direitos e liberdades fundamentais no que se refere ao tratamento dos dados pessoais" (Considerando 25 da Diretiva).

É importante ter em conta que essa partilha de dados deve ser feita de forma lícita, leal e transparente pois, se tais valores não forem respeitados, tal pode provocar prejuízos e até mesmo danos ao titular desses mesmos dados.

O próprio considerando n.º 51 da Diretiva expõe que "Os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderão resultar de operações de tratamento de dados suscetíveis de causar danos físicos, materiais ou morais, em especial caso o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a outros prejuízos importantes de natureza económica ou social (…) ".

Ou seja, as autoridades competentes quando acedem e tratam de dados pessoais de um individuo no contexto de uma investigação, devem fazê-lo de forma a garantir a segurança e confidencialidade dos mesmos. Dessa forma, evita-se que pessoas não autorizadas lhes acedam e os utilizem e os apliquem para outros fins.

Entende-se que esta Diretiva deve "andar lado a lado" com o Regulamento Geral sobre a Proteção de Dados (RGPD) (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho), que entrou em vigor a 24 de maio de 2016 e tem aplicação desde 25 de maio de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Nos termos do artigo 6.º da Diretiva deve-se fazer uma distinção clara entre diferentes categorias de titulares de dados, sendo os seus dados igualmente tratados de forma diferenciada. Assim, "Os Estados-Membros preveem que o responsável pelo tratamento estabeleça, se aplicável, e na medida do possível, uma distinção clara entre os dados pessoais de diferentes categorias de titulares de dados, tais como:

a) Pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal;
b) Pessoas condenadas por uma infração penal;
c) Vítimas de uma infração penal ou pessoas relativamente às quais certos factos levam a crer que possam vir a ser vítimas de uma infração penal;
d) Terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com

infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contactos ou associados de uma das pessoas a que se referem as alíneas a) e b).

Segundo o artigo 15.º, n.º 1 do mesmo diploma, "Os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;
b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais;
c) Proteger a segurança pública;
d) Proteger a segurança nacional;
e) Proteger os direitos e as liberdades de terceiros.

Quando um investigado e os seus atos parecem ter conexão com um país que não pertence à UE, é possível às autoridades competentes transferir os dados dessa pessoa para um então país terceiro ou até mesmo, para uma organização internacional. Nos termos do artigo 35.º, n.º 1 da Diretiva, tal transferência só se efetua quando:

i) A transferência for necessária para o cumprimento das finalidades previstas no n.º 1 do 1º artigo da Diretiva, ou seja, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública (alínea a);
ii) Os dados pessoais serem transferidos para um responsável pelo tratamento no país terceiro ou na organização internacional que seja uma autoridade competente para as finalidades referidas no artigo 1.º, n.º 1 (alínea b);
iii) Caso os dados pessoais sejam transmitidos ou disponibilizados por outro Estado-Membro, esse Estado ter dado o seu consentimento prévio à transferência nos termos do seu direito nacional (alínea c). Exceciona-se a

necessidade do consentimento prévio, caso este não consiga ser obtido em prazo útil e, seja possível prevenir uma ameaça imediata e grave à segurança pública de um Estado-Membro ou de um país terceiro ou aos interesses essenciais de um Estado-Membro (n.º 2 do artigo 35.º);

iv) A Comissão ter adotado uma decisão de adequação nos termos do artigo 36.º [isto é, a Comissão conseguiu determinar que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado, o que se mede face aos respeito por parte desse Estado pelos direitos humanos e liberdades fundamentais, entre outros] ou, na falta dessa decisão de adequação, terem sido apresentadas ou existirem garantias adequadas nos termos do artigo 37.º [garantias adequadas essas no que diz respeito à proteção de dados pessoais mediante um instrumento juridicamente vinculativo ou, o responsável pelo tratamento de dados tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados], ou, na falta de decisão de adequação nos termos do artigo 36.º ou de garantias adequadas nos termos do artigo 37.º, se forem aplicáveis derrogações a situações específicas nos termos do artigo 38.º [ou seja, tal transferência é passível de proteger os interesses vitais do titular dos dados ou de outra pessoa ou, para prevenir uma ameaça imediata e grave contra a segurança pública de um Estado-Membro ou de um país terceiro] (alínea d);

v) No caso de uma transferência ulterior para um país terceiro ou uma organização internacional, a autoridade competente que realizou a transferência inicial, ou outra autoridade competente do mesmo Estado-Membro, autorizar a transferência ulterior após ter em conta todos os fatores pertinentes, incluindo a gravidade da infração penal, a finalidade para que os dados pessoais foram transferidos inicialmente e o nível de proteção dos dados pessoais no país terceiro ou na organização internacional para os quais os dados pessoais são ulteriormente transferidos (alínea e).

3. A Lei n.º 59/2019, de 08 de Agosto

Aponto que a Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo responsável pela fiscalização do cumprimento do RGPD, da Diretiva e da Lei n.º 59/2019, de 08 de Agosto, que veio transpor essa última para o ordenamento jurídico português (artigo 43.º da Lei n.º 59/2019, de 08 de Agosto).

A CNPD é então, a entidade responsável em Portugal por acautelar e defender os direitos, liberdades e garantias que nos pertencem enquanto cidadãos, no âmbito do tratamento dos nossos dados pessoais. São «dados pessoais» as "informações relativas a uma pessoa singular identificada ou identificável" (artigo 3.º, n.º 1, alínea c) da Lei n.º 59/2019, de 08 de Agosto).

Aponto que, a CNPD é uma entidade administrativa. Controla, fiscaliza e aplica coimas. Se se tratar de um processo que envolva matéria criminal, o arguido responde em Tribunal.

Nesse sentido, essa Lei veio aprovar as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais.

Quanto ao regime em concreto da lei de transposição, no caso de alguém aceder indevidamente aos dados de outrem, sem qualquer autorização ou justificação, será punido com pena de prisão até um ano ou com pena de multa até 120 dias (artigo 53.º, n.º 1). Essa pena será agravada para o dobro nos seus limites quando o acesso for conseguido através de violação de regras técnicas de segurança (alínea a), do n.º 2 do artigo 53.º), quando tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial (alínea b), do n.º 2 do artigo 53.º) ou, tiver prejudicado inquéritos, investigações, processos judiciais ou a execução de sanções penais (alínea c), do n.º 2 do artigo 53.º).

Quem tiver copiado, subtraído, cedido ou transferido, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias (artigo 54.º, n.º 1). Mais uma vez, essa pena será agravada para o dobro nos seus limites nos casos já listados acima.

"Quem utilizar dados pessoais de forma incompatível com a finalidade determinante da respetiva recolha é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias" é isto que nos diz o artigo 55.º.

Quem violar o dever de sigilo a que está adstrito e nesse seguimento, sem justa causa e sem o devido consentimento, revelar ou divulgar, no todo ou em parte, dados pessoais tratados ao abrigo da presente lei, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias (artigo 58.º, n.º 1).

Tal pena será agravada para o dobro, caso o agente seja um funcionário ou equiparado, nos termos da lei penal, advogado ou solicitador (artigo 58.º, n.º 2, alínea a), caso o agente seja encarregado de proteção de dados (artigo 58.º, n.º 2, alínea b), caso o agente atue com a intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo (artigo 58.º, n.º 2, alínea c), caso o agente coloque em perigo a reputação, a honra ou a intimidade da vida privada de terceiros (artigo 58.º, n.º 2, alínea d) ou, caso o agente tenha prejudicado inquéritos, investigações, processos judiciais ou a execução de sanções penais (artigo 58.º, n.º 2, alínea e).

Quem não cumprir com os prazos fixados pela autoridade de controlo ou quem não colaborar com tal entidade, será punido com a pena correspondente ao crime de desobediência qualificada, ou seja, com uma pena de prisão até 1 ano ou com pena de multa até 120 dias (artigos 59.º, n.º 1 da Lei n.º 59/2019, de 08 de Agosto e 348.º, n.º 1 do Código Penal).

Outro diploma importante de mencionar é a Lei n.º 5/2002, de 11 de Janeiro que enquadra as medidas de combate à criminalidade organizada e económico-financeira, e que vem estabelecer "um regime especial de recolha de prova, quebra do segredo profissional e perda de bens a favor do Estado" relativamente a crimes como tráfico de estupefacientes, pornografia infantil e lenocínio de menores, contrabando, entre outros (artigo 1.º, n.º 1, alíneas a), l) e q) do referido diploma).

Segundo este diploma, "Nas fases de inquérito, instrução e julgamento de processos relativos aos crimes previstos no artigo 1.º, o segredo profissional dos membros dos órgãos sociais das instituições de crédito, sociedades financeiras, instituições de pagamento e instituições de moeda eletrónica, dos seus empregados e de pessoas que a elas prestem serviço, bem como o segredo dos funcionários da administração fiscal, cedem, se houver razões para crer que as respetivas

informações têm interesse para a descoberta da verdade" (artigo 2.º, n.º 1 do referido diploma).

No entanto, essa cedência depende "de ordem da autoridade judiciária titular da direção do processo, em despacho fundamentado" (artigo 2.º, n.º 2 do referido diploma). Esse despacho, vem identificar "as pessoas abrangidas pela medida e especifica as informações que devem ser prestadas e os documentos que devem ser entregues, podendo assumir forma genérica para cada um dos sujeitos abrangidos quando a especificação não seja possível" (artigo 2.º, n.º 3 do referido diploma).

No que concerne ao procedimento relativo a instituições de crédito, sociedades financeiras, instituições de pagamento e instituições de moeda eletrónica, o artigo 3.º, n.º 1 expõe que uma vez emitido o despacho mencionado acima, "a autoridade judiciária ou, por sua delegação, o órgão de polícia criminal com competência para a investigação, solicitam às instituições de crédito, às sociedades financeiras, às instituições de pagamento ou às instituições de moeda eletrónica as informações e os documentos de suporte, ou sua cópia, que sejam relevantes".

Essas instituições têm 5 ou 30 dias para fornecer os elementos requeridos, quanto a informações em suporte informático e quanto aos respetivos documentos de suporte e a informações não disponíveis em suporte informático. Este segundo prazo é reduzido caso os arguidos já se encontrem detidos ou presos (artigo 3.º, n.º 2 do referido diploma).

No caso destas instituições não cumprirem com os prazos estabelecidos ou ocultarem documentos ou informações "a autoridade judiciária titular da direção do processo procede à apreensão dos documentos, mediante autorização, na fase de inquérito, do juiz de instrução" (artigo 3.º, n.º 3 do referido diploma).

Se for necessário controlar os movimentos de uma conta bancária ou de conta de pagamento de um individuo, tal tem de ser autorizado ou ordenado por despacho do juiz e somente quando tiver grande interesse para a descoberta da verdade (artigo 4.º, n.º 2 do referido diploma).

Os membros dos órgãos sociais destas instituições "ficam vinculadas pelo segredo de justiça quanto aos atos previstos nos artigos 2.º a 4.º de que tomem conhecimento, não podendo, nomeadamente, divulgá-los às pessoas cujas contas

são controladas ou sobre as quais foram pedidas informações ou documentos" é isto que nos diz o artigo 5.º da Lei n.º 5/2002, de 11 de Janeiro.

O segredo de justiça está constitucionalmente consagrado no n.º 3 do artigo 20.º da Constituição da República Portuguesa (CRP) e encontra abrigo no artigo 86.º do Código de Processo Penal. O segredo de justiça implica que os atos de um processo não possam ser divulgados nem o público pode assistir aos mesmo. Este "visa, por um lado, garantir o sucesso da investigação (a obtenção de prova) e, por outro, proteger as partes envolvidas no processo, como o arguido (que, presumindo-se inocente, pode ver a sua honra e a sua privacidade injustificadamente atingidas) e a vítima".

Denoto que "nunca podem ser consultados os elementos relativos à vida privada de outra pessoa que não constituam meios de prova. Cabe à autoridade judiciária (Ministério Público ou juiz) especificar, em cada processo concreto, os elementos relativamente aos quais se mantém o segredo e, se for caso disso, ordenar a sua destruição ou a entrega à pessoa a quem dizem respeito".

O segredo de justiça corresponde então à "ablação ou restrição do conhecimento do processo ou de partes de um processo aos cidadãos em geral ou a certas pessoas em particular: radica aqui a distinção entre o segredo de justiça interno e o segredo de justiça externo que tem assento legal nos artigos 86.º a 90.º do CPP, aquele abrangendo os que são sujeitos e participantes do processo, que podem a ele aceder, mas não podem revelar o que conheceram"[351].

Na perspetiva penal, quando falamos dos procedimentos recolha, guarda, processamento, utilização e disseminação ou transferência de dados pessoais, temos de ter em conta que o titular dos dados foi em princípio, autor de uma infração ou vítima dela.

[351] BARREIROS, JOSÉ ANTÓNIO – "Segredo de Justiça e Conflito de Direitos: Espaço de Criminalização ou de Descriminalização?", Revista Julgar n.º 32 (2017), p. 190.

Conclusão

Exposto tudo o que se considerou de mais pertinente, é evidente que a expansão da sociedade da informação veio por si, facilitar a internacionalização da criminalidade, daí que seja tão relevante e tão atual, o tema deste artigo de opinião, relativo à "Legalidade do Acesso a Registos, Dados Cadastrais, Documentos e Informações em Sede de Investigações Criminais".

Devido a esta globalização das práticas criminosas, tornou-se ainda mais importante, os sistemas de cooperação jurídica internacional, especialmente no plano criminal, devido aos direitos violados que em princípio, estarão em causa.

"Neste sentido, as normas de proteção de dados pessoais devem aplicar-se também ao Estado quando coleta, manipula e difunde dados pessoais de investigados, suspeitos, réus, vítimas, testemunhas, peritos, autoridades e funcionários que atuam na persecução criminal e de terceiros eventualmente alcançados por medidas de apuração. Investigações criminais e medidas de segurança pública são atividades estatais que interferem rotineiramente na vida dos cidadãos, tornando-se relevante a perspetiva da privacidade"[352].

Assim o acesso a registos, dados cadastrais, documentos e informações está restringido ao que a Lei dispõe sobre tal, isto porque esses registos e demais elementos estão protegidos por leis de proteção de dados, que visam proteger a privacidade e os direitos das pessoas.

No entanto, em certas situações, esse acesso é permitido, mais uma vez reitera-se que só por lei tal é permitido, como no caso de investigações criminais, procedimentos legais, auditorias governamentais e outros casos semelhantes.

Estas ações de recolha, partilha, acesso e transferência de dados devem sempre ser realizadas de acordo com os procedimentos legais tendo como máxima, a proteção dos nossos direitos enquanto indivíduos. Isto significa que o acesso deve ser restrito apenas ao que é estritamente necessário, devendo as informações ser tratadas com o máximo de confidencialidade e segurança.

[352] ARAS, VLADIMIR – "A Título de Introdução: Segurança Pública e Investigações Criminais na Era da Proteção de Dados" *in* "Proteção de Dados Pessoais e Investigação Criminal", Editora ANPR, Brasília (2020), p. 25.

Conclui-se que, apesar de estar em causa o direito à reserva da intimidade da vida privada, a verdade é que este não é um direito absoluto, ou seja, pode ser limitado em certas situações.

Tal ocorre porque existem outros interesses e direitos que podem entrar em conflito com o direito à privacidade, como a segurança pública, a defesa nacional, a investigação criminal, entre outros.

Assim, nalguns casos, é possível que a privacidade seja relativizada ou mesmo suprimida em nome desses outros interesses, desde que sejam observados os limites estabelecidos pela lei e pelos princípios constitucionais.

É importante destacar que, apesar de não ser um direito absoluto, o direito à reserva da intimidade da vida privada é um direito fundamental e deve ser protegido pelo Estado e respeitado por todos, salvo nas situações em que sua limitação for estritamente necessária e proporcional.

Referências

Legislação

BRASIL, Presidência da República – Decreto-Lei nº 2.848, de 07 de Dezembro de 1940 - Código Penal brasileiro. Disponível em DEL2848compilado (planalto.gov.br)

BRASIL, Presidência da República, Lei 12.850/13, de 2 de agosto de 2013 - Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em L12850 (planalto.gov.br)

DIÁRIO DA REPÚBLICA. Decreto de 10 de Abril de 1976 - Constituição da República Portuguesa, Diário de República n.º 86/1976, Série I de 1976-04-10, páginas 738 – 775, Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-aprovacao-constituicao/1976-502635

DIÁRIO DA REÚBLICA, I Série, n.º 57/78, de 9 de Março de 1978 - Declaração Universal dos Direitos Humanos

DIÁRIO DA REPÚBLICA I, n.º 133, de 12/06/1978 (Lei n.º 29/78) – ONU - Pacto Internacional sobre os Direitos Civis e Políticos.

DIÁRIO DA REPÚBLICA. Decreto-Lei n.º 48/95, de 15 de Março - Código Penal português, Diário da República n.º 63/1995, Série I-A de 1995-03-15, páginas 1350 – 1416, Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/48-1995-185720

DIÁRIO DA REPÚBLICA n.º 9/2002, Série I-A de 2002-01-11, páginas 204 – 207 - Lei n.º 5/2002, de 11 de Janeiro - Estabelece medidas de combate à criminalidade organizada e económico-financeira e procede à segunda alteração à Lei n.º 36/94, de 29 de Setembro, alterada pela Lei n.º 90/99, de 10 de Julho, e quarta alteração ao Decreto-Lei n.º 325/95, de 2 de Dezembro, alterado pela Lei n.º 65/98, de 2 de Setembro, pelo Decreto-Lei n.º 275-A/2000, de 9 de Novembro, e pela Lei n.º 104/2001, de 25 de Agosto. Disponível em https://diariodarepublica.pt/dr/detalhe/lei/5-2002-583017

DIÁRIO DA REPÚBLICA. Resol. da AR n.º 32/2004, de 02 de Abril - Aprova, para ratificação, a Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, o Protocolo Adicional Relativo à Prevenção, à Repressão e à Punição do Tráfico de Pessoas, em especial de Mulheres e Crianças, e o Protocolo Adicional contra o Tráfico Ilícito de Migrantes por Via Terrestre, Marítima e Aérea, adoptados pela Assembleia Geral das Nações Unidas em 15 de Novembro de 2000.

DIÁRIO DA REPÚBLICA. Lei n.º 59/2019, de 08 de Agosto - Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Diário da República n.º 151/2019, Série I de 2019-08-08, páginas 41 – 68, Disponível em https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, 04 de maio de 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680

TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM – Conselho da Europa - Convenção Europeia dos Direitos Humanos de 02/04/2013.

Artigos

BADARÓ, GUSTAVO – "Processo Penal e Criminalidade Organizada", Colóquio de Direito Luso-Brasileiro, Faculdade de Direito do Largo de São Francisco – USP/Faculdade de Direito da Universidade de Lisboa (12 a 16 de Maio de 2014);

BITENCOURT, CEZAR ROBERTO – "Sonegação de Informações Requisitadas", R. EMERJ, Rio de Janeiro, v. 18, n. 67 (2015);

BARREIROS, JOSÉ ANTÓNIO – "Segredo de Justiça e Conflito de Direitos: Espaço de Criminalização ou de Descriminalização?", Revista Julgar n.º 32 (2017);

ARAS, VLADIMIR – "A Título de Introdução: Segurança Pública e Investigações Criminais na Era da Proteção de Dados" *in* "Proteção de Dados Pessoais e Investigação Criminal", Editora ANPR, Brasília (2020).

Links:

https://manhez.jusbrasil.com.br/artigos/825703966/organizacao-criminosa-lei-12850-13-acao-controlada-infiltracao-de-agentes-e-acesso-a-registros – acedido a 14/10/2023;

https://www.pgdporto.pt/proc-web/faq.jsf?ctxId=85&subCtxId=94&faqId=1050&show=&offset – acedido a 16/10/2023;

https://dre.pt/dre/lexionario/termo/segredo-justica – acedido a 17/10/2023;

https://ffms.pt/pt-pt/direitos-e-deveres/quando-um-processo-penal-se-encontra-sob-segredo-de-justica-este-segredo-abrange – acedido a 19/10/2023;

http://www.sermais.pt/media/86/File/VIHDireito/HIV_Direito_Reserva_Sobre_Intimidade_Vida_Privada.pdf – acedido a 20/10/2023.

Lei Geral de Proteção de Dados e o Direito ao Esquecimento nas Redes Digitais, Análise Constitucional Comparada

Débora de Abreu Moreira dos Santos Martins[353]

Marcilete Cardoso da Silva [354]

Resumo

O objetivo do presente artigo é analisar o denominado direito ao esquecimento, no âmbito das relações digitais, como meio de preservação da privacidade do indivíduo de acordo com Constituição da República Federativa do Brasil de 1988 atualizada, no contexto das garantias e direitos fundamentais, em especial o direito à privacidade e à dignidade da pessoa humana. As normas infra legais, como o Código Civil brasileiro, remetem aos direitos da personalidade, elemento essencial para entender como efetivar o direito ao esquecimento. Foi realizado um exame do direito internacional, em especial a Regulamentação Geral de Proteção de Dados da União Europeia (GDPR), para a criação e efetivação da Lei Geral de Proteção de Dados (LGPD) no âmbito da proteção dos dados digitais dos cidadãos. Inúmeros casos concretos são abordados e contrastados com a legislação pátria e com o entendimento jurisprudencial das Cortes Superiores. A análise doutrinária busca consolidar e aprofundar o tema do "direito ao esquecimento". Não obstante, a sociologia e a filosofia são chamadas para traçar os parâmetros de causa e efeito, quando da não efetivação deste direito. Portanto, conclui-se que, embora a

353 Doutora em Psicologia pela Pontifícia Universidade Católica de Goiás, Mestre em Direito Internacional Economico pela Universidade Católica de Brasília, atualmente Professora de Graduação do Centro Universitário de Goiás (UNIGOIÁS). Coordenadora e professora do curso de pós-graduação em Psicologia Jurídica da PUCGO, e-mail: martins184@gmail.com

354 Especialista em Lei Geral de Proteção de Dados. Professora de Pós-Graduação da Faculdade Unida de Campinas – FacUnicamps e autora de livro. Advogada, membro da Comissão de Direito Digital e Informática (CDDI) da Ordem dos Advogados do Brasil – Seção Goiás (*OAB-GO*), e-mail: marciletecardosoadv@gmail.com

legislação brasileira, ao positivar tal direito, seja falha ao tratar de forma taxativa o tema, não existe a negação de sua existência e as recentes decisões do Supremo Tribunal Federal estão longe de pacificar a discussão, que se represa conforme o tempo fluí, deixando a cargo da sociedade, por meio de seus representantes devidamente eleitos, a elaboração de políticas públicas de Estado, como forma de positivar em lei o referido direito.

Palavras-chave:
Redes sociais; LGPD; GDPR; Garantias fundamentais.

Introdução

O estudo busca demonstrar a importância em analisar o direito ao esquecimento considerando o desenvolvimento humano no contexto da era virtual, na sociedade do século XXI, pós evolução digital, uma vez que, a sua (in)aplicabilidade, corresponde em uma situação de risco a dignidade da pessoa humana, qual não pode ser deletada, induzindo a construção de críticas públicas incontroláveis.

Os direitos fundamentais vislumbram proteger o direito do cidadão, intelectual, financeira e socialmente. Cabendo ao Estado, proteger tal direito. Entende-se do artigo 11º, item 2, do *Pacto de San José da Costa Rica, in verbis:*

> Artigo 11 - Proteção da honra e da dignidade
> 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas." (Tratado Internacional - Convenção Americana de Direitos Humanos - Pacto de São José da Costa Rica, 1969)

Para BAUMAN (2001), p.96, a existência de pós-modernidade não se concatena com a realidade expressa. Demonstra, na verdade, que há uma série de elementos e situações fáticas que se reciclam na modernidade, como o consumismo, que não mais se expressa na satisfação das necessidades. Demonstrando um mundo "líquido" e dinâmico em suas relações sociais e comportamentais.

O próprio individuo, em razão da velocidade das mudanças comportamentais, não consegue compreender o risco e o dano causado por suas ações e posições, em um mundo onde nada é esquecido, apenas guardado para o momento correto. Em décadas passadas, à juventude era permitido errar e aprender com os erros. Hoje, os jovens crescem em um ambiente onde o erro não será esquecido. Daí surge a necessidade de atuação do Estado, para resguardo de seu direito.

No começo do ano de 2018, em reportagem da revista "Estado de São Paulo", o governo federal rescindiu contratos com terceirizados e comissionados em razão de publicações em redes sociais, pré-campanha eleitoral, defendendo

posicionamentos políticos. Apartado das paixões políticas, o que se demonstra é que, estas pessoas nada fizeram para ensejar tal desprezo senão a de publicarem seus posicionamentos políticos, algo que a própria constituição federal assegura. Embora muitos destes cargos sejam de livre nomeação, os princípios que regem a administração pública, em especial o da isonomia, são postulados que visam resguardar direitos fundamentais em razão de quem preside respectivo cargo.

A implementação do Marco civil da internet fora um esforço para começar a tratar desses desafios da modernidade. Apesar de, há muito pouco gestado, o diploma veio, ao longo do tempo, sendo melhorado, por meio de decretos legislativos e executivos sobre o tema, o que culminou na criação da Lei Geral de Proteção de Dados.

Dentre as diretrizes deste novo diploma normativo, está o direito ao esquecimento. Não no sentido tratado por FOUCAULT (1987), p.31, na obra "Vigiar e Punir", mas sim na situação das relações privadas dos indivíduos, permitindo aos cidadãos, gozar de livre pensamento, sem represálias sobre suas posições: políticas; religiosas etc.; ou até mesmo ocultar atos pretéritos que hoje não mais constituem a personalidade intelectual e social do indivíduo.

1 - A constitucionalidade da privacidade

A Constituição da República Federativa do Brasil de 1988 (CRFB/88), inovou ao tratar em seu artigo 5º sobre os direitos fundamentais do cidadão, razão pela qual foi denominada constituição cidadã. Nesse sentido, tendo como palco a análise do "direito ao esquecimento", nos aspectos das relações civis, há de se averiguar se a Carta Magna protege, nos dias de hoje, a privacidade de seus cidadãos contra terceiros e principalmente contra o Estado.

A validade jurídica do direito ao esquecimento, não se confunde com o advindo do direito penal, que versa sobre o cumprimento da sanção penal e a reintegração do indivíduo à coletividade, não perpetuando os efeitos da pena cumprida. A análise do artigo vislumbra discutir a proteção das garantias individuais, em especial ao direito à privacidade, postulado primário daquilo que se entende como direito ao esquecimento, ora no aspecto constitucional, ora nas questões suscitadas pelo direito constitucional comparado presente nos tratados internacionais que versam sobre o referido tema.

1.1 - Direito a privacidade como um direito fundamental na CRFB/1988

O art. 5º, caput em consonância com seu inciso X, apresenta à proposta do legislador constituinte na proteção do Direito a privacidade do cidadão, sendo importante a sua transcrição:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, Brasília, DF: Presidência da República, [2020])

Dessa forma, a aplicação da referida norma, em um contexto de alta interligação computacional, como bem pontua Castells (1999): "um mundo em redes"; a privacidade do indivíduo, deixa a esfera privada e passa a ser, o que Doneda (2010) observou, "mercadoria".

Destarte, ficou a cargo dos legisladores, a criação de normas reguladoras a fim de efetivar tais garantias constitucionais. No âmbito das relações comerciais, tal proteção constitucional, pode ser encontrada no inciso XXXII, do art. 5º da CF/88, onde, "o Estado promoverá, na forma da lei, a defesa do consumidor".

Em que pese, à época, o constituinte não ter incorporado tal norma, no sentido da proteção dos dados do cidadão, nada obsta a sua interpretação no sentido da proteção à intimidade do indivíduo.

Nesse sentido, os tribunais têm dado a interpretação de que, as empresas que utilizam dados de seus usuários, ou adquiridos mediante base de dados de outrem, para ofertar produtos, praticam invasão da privacidade e do sossego, devendo indenizar pelo dano causado, como pode ser extraído do julgado do Tribunal de Justiça do Distrito Federal e Territórios:

> EMENTA: DIREITO DO CONSUMIDOR. FALHA NA PRESTAÇÃO DE SERVIÇOS. SEGURANÇA DA INFORMAÇÃO. ANÚNCIO EM SITE DE CLASSIFICADOS ONLINE. PÁGINA DE ACOMPANHANTES. DANOS MORAIS. VALOR DA INDENIZAÇÃO. 1. Na forma do art. 46 da Lei 9.099/1995, a ementa serve de acórdão. Recurso próprio, regular e tempestivo. 2. Falha na prestação de serviços. Nas relações de consumo, responde o fornecedor objetivamente por eventuais danos causados ao consumidor decorrentes de falha na prestação dos serviços, na forma do art. 14 do Código de Defesa do Consumidor.

> Ainda, em seu §1º, "O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar[...]". Caracteriza falha na prestação de serviços a disponibilização de anúncio em site de classificados online sem a verificação da autenticidade e identidade do anunciante, a fim de evitar possíveis fraudes, principalmente em anúncios de acompanhantes onde a pessoa que está oferecendo seus serviços não costuma divulgar seus dados pessoais como, no caso, o nome completo. 3. Responsabilidade civil. Dano Moral. O dano causado à autora é evidente, considerando que seu nome, sobrenomes e telefones, inclusive profissional, de atividade completamente distinta, foram disponibilizados em site de classificados online, como anúncio de acompanhante. A autora demonstra que seus dados pessoais foram expostos e que foi atingida em seus atributos da personalidade, de modo que é cabível indenização por danos morais. De outra parte, não resta caracterizada a culpa exclusiva de terceiro a romper o nexo causal, pois foi a inadequada prestação de serviços da ré, sem os cuidados que a especificidade requer, que permitiu a indevida veiculação de anúncio que atingiu a intimidade e a imagem da autora, de modo que resta caracterizada a sua responsabilidade pelo ilícito. 4. Valor da indenização. O valor fixado na sentença para a indenização (R$10.000,00) cumpre com adequação as funções preventivas e compensatórias da condenação. Sentença que se confirma pelos seus próprios fundamentos. 5. Litigância de má-fé. A omissão da ré na produção de provas em seu favor não caracteriza litigância de má-fé. Antes revela o simples desinteresse na defesa, que é sancionada com as consequências decorrentes do ônus imposto pela Lei. Recurso a que se dá parcial provimento para afastar a condenação por litigância de má-fé. 6. Recurso conhecido, e provido, em parte. Custas processuais e honorários advocatícios, fixados em 10% do valor da condenação, pelo recorrente vencido. (Acórdão n. 971472, Relator Juiz AISTON HENRIQUE DE SOUSA, 2ª Turma, Data de Julgamento: 5/10/2016, publicado no DJe: 13/10/2016) (TJ-DF, 2016).

Por outro lado, em matéria similar, o entendimento se mostra controverso e ainda não consolidado, ficando a cargo de cada juízo, a interpretação ao caso concreto sobre o dano ocasionado, conforme se extraí do julgado do Tribunal de Justiça de Santa Catarina:

> EMENTA: APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA C/C INDENIZAÇÃO POR DANOS MORAIS. SISTEMA "CREDIT SCORING". JULGAMENTO LIMINAR DO PROCESSO, COM FULCRO NO ART. 285-A DO CPC/73. INSURGÊNCIA DA AUTORA. PEDIDO DE EXCLUSÃO DO SISTEMA "SCORE", SOB A ALEGAÇÃO DE AUSÊNCIA DE NOTIFICAÇÃO. TESE RECHAÇADA. SUPERIOR TRIBUNAL DE JUSTIÇA QUE RECONHECE A LICITUDE DO REFERIDO SISTEMA, QUE NÃO CONSTITUI CADASTRO OU BANCO DE DADOS, MAS TÃO SOMENTE UM MODELO ESTATÍSTICO. NÃO COMPROVADO O ABALO DE CRÉDITO OU OUTRO PREJUÍZO. DESNECESSIDADE DO CONSENTIMENTO PRÉVIO E EXPRESSO DO CONSUMIDOR. DANO MORAL NÃO CONFIGURADO. SENTENÇA MANTIDA. "1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). 2) Esta prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do castro positivo). 3) Na avaliação

> do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção ao consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. 4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. 5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados, incorretos ou desatualizados" (Resp 1419697/RS, Rel. Ministro Paulo de Tarso Sanseverino, Segunda Seção, julgado em 12/11/2014, DJe 17/11/2014). RECURSO CONHECIDO E DESPROVIDO. (TJ-SC - AC: 03245282520148240023 Capital 0324528-25.2014.8.24.0023, Relator: José Agenor de Aragão, Data de Julgamento: 19/09/2019, Quarta Câmara de Direito Civil) (TJ-SC, 2019)

Observa-se que a proteção do direito ao esquecimento é demasiadamente extensa, ainda mais quando contrastado com a realidade de um "mundo líquido" (BAUMAN, 2001) e "interligado em redes" (CASTELLS, 1999), onde o cidadão encontra-se em constante violação de seus direitos, embora ele mesmo não tenha ideia de tal violação. Nesse sentido, cabe, inicialmente, a propositura de uma diferenciação no que concerne a direitos fundamentais e garantias fundamentais, para que se possa chegar a um mínimo denominador comum, sobre o tema.

Nas lições de LENZA (2020), P.252, essa diferenciação entre, garantias e direitos fundamentais, se faz na seguinte medida: "[...]os direitos são bens e vantagens prescritos na norma constitucional, enquanto as garantias são os instrumentos através dos quais se assegura o exercício dos aludidos direitos (preventivamente) ou prontamente os repara, caso violados". Diante desse contexto, a privacidade, como princípio, é antes de tudo uma garantia e um direito fundamental, de sorte que, a violação à privacidade do indivíduo, vem assegurada de instrumentos jurídicos capazes de fazer cessar, preventivamente ou prontamente, a transgressão.

Nesse aspecto, o direito à privacidade é imperativo categórico para efetivação do princípio da dignidade da pessoa humana. Todavia, há de se ressaltar que, tanto a privacidade, quanto outros direitos, quando em situações de confronto de normas, deve-se optar pelo princípio da proporcionalidade, como fonte

balizadora, cabendo ao Poder Judiciário, estabelecer os limites de um direito e garantia em detrimento de outro. Assim, para, BARRETO (2010), p. 62, o entendimento de dignidade humana é de relevância jurídica ímpar, atuando como fonte de todos os demais direitos individuais, inclusive com força de interpretação abrangente atingindo questões em que nenhum outro princípio ou conceito jurídico possa ser utilizado.

Desse entendimento sobre o direito à privacidade, como garantia fundamental, quando em choque com outros direitos e garantias fundamentais, como: a liberdade de expressão; a livre manifestação do pensamento e à livre imprensa, nasce o que se convencionou chamar "direito ao esquecimento".

Muito embora o Supremo Tribunal Federal ao enfrentar o tema, no início do ano de 2021, tenha firmado entendimento de que é incompatível com a Constituição Federal um "direito ao esquecimento" que tenha por fim, obstar fatos pretéritos e notórios, de interesse público, o que se extraí dos votos dos eminentes ministros, é a necessidade de se verificar as condições existentes para a liberdade de imprensa e do livre pensamento, e quando estas invadem a esfera privada do indivíduo, nada obsta ao poder judiciário, sua mitigação e deferimento, ou não, dos elementos que compõem o "direito ao esquecimento".

É diante desse macrocenário judicial, onde o choque de normas constitucionais com o direito à privacidade, que o "direito ao esquecimento" ganha seus contornos e vai se consolidando, na medida em que as demandas da sociedade, vão sendo assentadas nos entendimentos jurisdicionais.

2- O atual direito ao esquecimento no ordenamento Jurídico Brasileiro

Conforme observado, o chamado "direito ao esquecimento", trata-se de uma construção doutrinária, tendo como norte a congregação de outros direitos, relacionados à normas constitucionais, em especial o direito à dignidade da pessoa humana e o direito à privacidade, bem como os direitos da personalidade elencados no Código Civil Brasileiro.

Muito embora, *a priori*, tal direito seja, em essência, um direito subjetivo, nada obsta a sua aplicação. Ao contrário, o fato de o legislador não ter atribuído, à época, a devida expressão, ora tratada, para versar sobre esse tema, não significa sua inexistência no âmbito jurídico.

A perseguição jurídica por ações que regulamentem o setor de comunicações digitais, em especial no quesito do tratamento de dados, fez a pressão necessária para que o país, por meio de seus representantes legais, iniciasse o debate e a efetivação de normas legais. Com o advento da Lei 12.965/2014, comumente denominada de Marco Civil da Internet, criou-se o básico para a consolidação de direitos e garantias fundamentais no âmbito das relações digitais.

Ciente que no contexto, no internacional para a regulamentação e criação de legislações que versam sobre os direitos e garantias na internet, em especial a União Europeia, com a criação do Regulamento (UE) 2016/679, de 27 de abril - Regulamento Geral de Proteção de Dados (RGPD), fora o impulso necessário para a criação de uma legislação nacional, inspirada no referido diploma legal, nascendo assim a Lei 13.709/2018, doravante denominada Lei Geral de Proteção de Dados.

2.1 - O diálogo jurídico entre o direito ao esquecimento com o direito internacional europeu

Nessa esteira de acontecimentos e mudanças da legislação, a introdução da Lei Geral de Proteção de Dados (Lei 13.709/18) trouxe em seu bojo a especificação do que se entende por direitos do titular dos dados no âmbito digital; em especial em seu artigo 17, apesar de não trazer expressamente o termo "direito ao esquecimento", converge para o que se versa no entendimento das garantias e direitos fundamentais.

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. (BRASIL, 2018)

A citada legislação traz em seu inciso XIV do artigo 5º, o direito de eliminação como sendo a "exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado". Com efeito, parece não ser possível extrair da Lei Geral de Proteção de Dados (Lei 13.709/18), qualquer relação entre o Direito à Eliminação de Dados e o Direito ao Esquecimento. Examina-se que o direito de ser "esquecido", na LGPD, é na verdade o direito que o titular de dados tem de solicitar, a qualquer momento, a eliminação de suas informações

pessoais da base de dados de uma empresa ou organização (agentes de tratamento).

Quanto contrastada com leis estrangeiras, em especial o RGPD, da União Europeia, percebe-se claramente que o legislador adentrou ao tema, adotando a nomenclatura, para fins de dirimir, na medida do possível, quaisquer interpretações adversas. O RGPD expressa em seu artigo 17º, que trata do direito de apagar dados, seguido do subtítulo "direito ao esquecimento". Dessarte, o artigo 66º, da mesma norma, também contém a descrição de "direito ao esquecimento no meio eletrônico" (UNIÃO EUROPÉIA, 2020).

> Artigo 17. Direito ao apagamento dos dados («direito a ser esquecido»)
> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: (UNIÃO EUROPÉIA, 2020)

Nesse sentido, a pressão internacional por políticas que visam a privacidade do indivíduo nas redes, começaram, timidamente, a serem positivadas em nosso ordenamento jurídico. Em que pesem as normas de proteção ao direito ao esquecimento, serem demasiadamente genéricas e de difícil aplicação, no âmbito das relações digitais, observa-se que passos necessários foram dados.

A Lei Geral de Proteção de Dados busca atender a essa demanda, não só internacional, como da própria sociedade brasileira, na medida em que busca efetivar a responsabilização dos agentes detentores dos dados, quando utilizados de maneira indevida, e garante ao titular, o direito de ter acesso àquilo que lhe pertence, bem como a exclusão de seus dados pessoais, quando passíveis de serem excluídos, uma vez que tal direito não é absoluto.

Todavia, tal proteção ainda carece de uma maior concretização, e, na medida do que se observa, verifica-se os seus consideráveis desafios, uma vez que trata-se de uma mudança cultural tanto para as organizações (empresas e governo) quanto para o cidadão comum, em especial a este que, em sua grande maioria, sequer tem a real noção do risco, quanto permite a coleta e o compartilhamento de seus dados, com o sem a sua anuência.

2.2 - Conflitos jurídicos no Direito ao Esquecimento entre decisões constitucionais e dissonâncias nas Instâncias Superiores

Para uma melhor compreensão do quadro deletério, é oportuna a citação do caso ocorrido nos Estado Unidos, no ano de 2006, retratados na obra: "*Delete – The Virtue of Forgetting in the Digital Ace*"; do pesquisador e professor Victor Mayer Shönberger, onde traz o caso "*Drunk Pirate*" (Pirata Bêbada).

Stacy Snayder, uma mãe solteira de dois filhos, acabara de concluir seu curso e estava em busca de uma carreira como professora iniciante. Porém, as autoridades responsáveis da universidade lhe negaram seu certificado, embora tenha concluído todas as matérias. A justificativa foi a de que seu comportamento pessoal era incompatível com o exercício da carreira de professora, pois fora publicada em uma rede social, uma foto de Stacy, fantasiada de pirata, segurando um copo de plástico, com a descrição de "pirata bêbada". A universidade ainda notificou os professores a respeito do ocorrido, alertando que tal comportamento não era profissional. Stacy ainda cogitou remover a postagem, porém, o dano já havia sido causado.

Mais tarde Stacy Snayder processou a universidade, alegando que a postagem de uma foto de um evento privado, em uma rede social, aludindo que poderia estar – ou não – sob influência de álcool, não a desabonava para efetivar a conclusão e certificação de seu curso. Entretanto, a demanda judicial não prosperou em favor de Stacy e manteve os efeitos administrativos impostos pela referida universidade.

O problema, como bem aponta (SCHOMBERGER, 2009), vai muito além da negativa da emissão do certificado pela universidade. Desde os primórdios, as sociedades tinham como regra o esquecimento e a lembrança como exceção e essa balança se inverteu nas últimas décadas.

No Brasil, dois casos específicos ganharam destaque ao tratar do direito ao esquecimento, muito embora, ambos não versem especificamente sobre o meio digital, é impossível tal desvinculação, haja vista que a potencialização e a perpetuação estão contidas em tal meio.

O primeiro caso é o da família Curi, enfrentado pelo Supremo Tribunal Federal em fevereiro de 2021. Trata-se de Recurso Especial n. 1.010.606/RJ, com repercussão geral, onde os familiares de Aída Curi, pleiteavam, em desfavor da emissora de

televisão Globo, solicitando reparação civil pela encenação do assassinato de Aída Curi, em 1950, no Rio de Janeiro, sem autorização expressa da família, sob a alegação de que os autores, irmãos de Aída Curi, tinham o direito de esquecer as brutalidades que fora submetida a vítima e a dor constante, ocasionada pela relembrança do fato passado.

Nesse sentido, o Supremo Tribunal Federal, seguiu, em sua maioria, o entendimento do voto do Ministro Relator Dias Toffoli, que rejeitou a tese do direito ao esquecimento, em detrimento do direito à livre imprensa e informação. Ressaltou o Ministro Relator que a LGPD: "pretendeu cercar os dados de ampla proteção, viabilizando meios para eventuais correções que se façam necessárias". Todavia, a referida lei "não trouxe um direito ao indivíduo de se opor a publicações nas quais dados licitamente obtidos e tratados tenham constado" que este silêncio, não obstante, deriva-se de mandamentos constitucionais.

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. (STF, 2021)

Complementa o nobre relator que:

> Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais — especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral — e as expressas e específicas previsões legais nos âmbitos penal e cível. (STF, 2021)

O segundo caso, de ampla repercussão nacional, foi enfrentado pelo Superior Tribunal de Justiça, no Recurso Especial n. 1.334.097/RJ, conhecido como "chacina da candelária", onde adolescentes desabrigados, que dormiam em frente à igreja Nossa Senhora da Candelária, no ano de 1993, no Rio de Janeiro, foram assassinados, aparentemente, por um grupo de policiais e um serralheiro.

Em reprise, apresentada pelo programa linha direta, da emissora Rede Globo, fora apresentada uma entrevista com o serralheiro, Jurandir Gomes de França, absolvido pelo tribunal do júri à época, e veiculando de forma indireta, seu nome como um dos partícipes. Todavia, o Superior Tribunal de Justiça entendeu que a menção de seu nome constituiu grave dano à honra do impetrante, reconhecendo em decisão colegiada, o direito ao esquecimento do autor. Dessarte, oportuno se faz a menção do trecho do voto do relator:

> Desse modo, o antigo conflito entre o público e o privado ganha uma nova roupagem na modernidade: a inundação do espaço público com questões estritamente privadas decorre, a um só tempo, da expropriação da intimidade/privacidade por terceiros, mas também da voluntária entrega desses bens à arena pública.
> Constroem-se "amizades" em redes sociais em um dia, em número superior ao que antes se construía em uma vida.
> Porém, sem nenhuma dúvida, mais grave que a venda ou a entrega graciosa da privacidade à arena pública, como uma nova mercadoria para o consumo da coletividade, é sua expropriação contra a vontade do titular do direito, por vezes um anônimo que pretende assim permanecer. (STJ, 2013)

Nitidamente, há uma dissonância de entendimentos entre a Corte Constitucional e o Tribunal da Cidadania acerca dos casos mencionados. A falta de pacificação - seja em razão do silêncio da norma, seja em razão do caso concreto analisado -, em diversas outras causas, traz inúmeros prejuízos aos juízos e tribunais de instância inferior ao enfrentar o tema.

Fica evidente que os aparatos legais não estão disponíveis a todos. Embora a discussão esteja em voga, os casos estão acumulando de forma exponencial e, em que pese a criação de diplomas legais, que versem sobre o assunto, inúmeras variáveis conspiram contra sua aplicação, quer seja pela falta de clareza no texto legal, quer seja pela interpretação, ainda subjetiva de cada juízo. Destarte, se observa que tal proteção não pode ser alcançada apenas com a legislação vigente. Há a necessidade de que o Poder Público, adote políticas que visem coibir a utilização desenfreada de exposição dos usuários.

3. A necessidade de políticas públicas para garantir a proteção aos direitos individuais no mundo digital

Conforme foi apresentado no tópico anterior, a insuficiência concreta de proteção, no que persegue a dignidade da pessoa humana, como relatada nos casos concretos, deixa ainda o cidadão em uma situação de risco, uma vez que seus dados e sua trajetória estão armazenados e disponíveis, de forma lícita ou não, a quem convém fazer sua utilização.

Em virtude dessa proteção insuficiente, surge a necessidade de implementação de políticas públicas, como forma de corrigir as distorções

ocasionadas tanto pelo engessamento do sistema judiciário, ao lidar com o tema, quanto pelas regras de mercado, quando lidam de forma indevida com dados privados de seus usuários.

A necessidade de se criar uma política pública de Estado (FORTINE, ESTEVES e DIAS, 2008), que independe do governo ou governante, pautada nos ditames constitucionais, é razão urgente para fazer cessar o dano em relação ao indivíduo. Principalmente pelo fator político, que uma política pública de governo pode acarretar, podendo vir a privilegiar aliados ideológicos e políticos em detrimento daqueles que constituem oposição ao governo de plantão.

É perceptível, que os meios legais existentes com o intuito de garantir a proteção de informações pessoais, em especial, no âmbito digital, são ainda incipientes e pouco acessíveis aos que demandam judicialmente para efetivar seus direitos. As plataformas de redes sociais, atualmente são parte intrínseca do cotidiano da sociedade e suas diretrizes são traçadas na obtenção de lucro – como toda empresa.

No tocante às inovações quanto ao tratamento de dados, inclusive no meio digital, trazido pela LGPD, após pouco mais de três de vigência da referida legislação, ainda se verifica que a forma como os termos e diretrizes de utilização dos dados pessoais são apresentadas aos seus usuários é de difícil compreensão e por vezes não possibilita a sua escolha em aderir ou não aos termos estabelecidos na plataforma.

Com efeito, as grandes empresas de comunicação digital estão a fazer as vezes do Estado, delimitando, na medida de seus interesses, suas regras, às margens da Constituição da República e das leis, ditando o que pode e o que não pode ser feito. Esse sistema autopoiético é bem ilustrado por Niklas Luhmann, ao tratar do sistema e o meio ambiente.

> A sociedade constitui-se de unidades elementares (comunicações), e tudo o que se forma dessa maneira, volta para a sociedade e torna-se um ponto no processo da sua formação. Neste sistema, as consequências são inevitáveis mesmo as negativas, elas estão incluídas e servem, se não a preservação das estruturas, ao menos, para conservar a reprodução autopoiética da mesma. Assim, a empresa pode ser vista como uma ordem auto-substitutiva, uma vez que tudo o que é necessário para alterar ou substituir nela, tem de ser alterado ou trocado dentro dela. (LUHMANN, 1992, p. 14)

Nesse sentido, a proposição trazida por Niklas Luhmann, quando trata do "risco", se faz presente, mediante a propositura de projetos, pelo Poder Legislativo,

notadamente, que versam sobre o direito ao esquecimento, na medida em que um dos determinados subsistemas, dentro do sistema social, quando tensionado, força os demais a gerarem uma solução para equalizar o ambiente.

3.1 - Direito ao esquecimento - Políticas Públicas na Câmara Legislativa

Em que pese o Supremo Tribunal Federal, no julgamento das ações supracitadas, firmar entendimento de que não existe "direito ao esquecimento" no ordenamento constitucional, a sociedade, por meio de seus representantes eleitos, busca, na medida em que o problema se agrava, as vias democráticas e de direitos possíveis para solucionar o risco iminente a que se está submetido.

A percepção de que os prejuízos advindos da coleta e armazenamento dos dados de cada passo do indivíduo, com a finalidade de lucro, gera não apenas uma situação de risco individual, mas também coletivo. Esse risco é repassado ao custeio do Estado, quando as vias judiciárias são acionadas para solucionar conflitos desta natureza.

O "risco" nasce não apenas da evolução das tecnologias e comportamentos da sociedade moderna, mas também quando o Estado deixa de criar mecanismos de freios e contrapesos para solucionar possíveis dissídios, potencializando esses riscos e aumentando os gastos com a máquina pública, seja para custear o acionamento do poder judiciário, seja para amenizar os danos já ocasionados em face do coletivo.

O risco que se menciona é o trazido por Adams (2009), na obra "Risco", ao tratar da "sociedade de risco" de BECK (2011), p. 250 – 251: "hoje em dia, muito mais riscos são da competência do governo e das grandes corporações. Em comparação com épocas anteriores e menos complexas em termos de tecnologia, um número muito maior de decisões sobre o risco foi assumido por legisladores, regulamentadores e profissionais especializados em segurança".

Iniciativas legislativas, no momento, procuram sanar essas lacunas. Atualmente, tramitam, apenas na Câmara Legislativa doze projetos de lei, que abrangem o tema. Entretanto, impossível não observar que existem projetos que versam sobre o tema desde 2014, sem o efetivo andamento. Dentre essas medidas, observa-se que muitas possuem o mesmo fundamento, alterando, em partes, o

alcance do direito a ser pleiteado, o direito ao esquecimento. Nesse contexto, cabe destacar dois projetos que merecem monitoramento legislativo.

3.2 - Projeto de Lei 4306/2020 – direito ao esquecimento – estatuto da criança e do adolescente

O Projeto de Lei 4306/2020, apresentado em 25/08/2020 pelo Dep. Lídice da Mata - PSB/BA, cuja ementa segue abaixo, visa trabalhar o direito ao esquecimento na esfera da proteção à criança e adolescente, vítimas ou testemunha de violência, podendo solicitar a exclusão dos dados pessoais de sites de pesquisa ou de notícias.

Observa-se que há uma preocupação do direito ao esquecimento, quando se confronta o direito à informação com o direito à privacidade da criança ou adolescente. Segundo o relator do projeto, o resultado pernicioso da utilização desses dados, remete à revisitação constante da violência pelo ofendido. Destarte, que as chagas perpetuariam no tempo sem possibilidade de cicatrização.

> EMENTA: Altera a Lei 13.431, de 4 de abril de 2017, que estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência, para prever o direito da criança ou adolescente de pleitear a exclusão de informações pessoais de sites de pesquisa ou de notícias que possam causar-lhe constrangimentos ou danos psicológicos e dá outras providências. (BRASIL, 2020)

Em que pese a vulnerabilidade em razão da idade, há clara semelhança da tutela pretendida com os casos narrados neste trabalho, ainda que em medidas e graus distintos. Não se busca uma equidade em relação à pessoa em si, mas à condição temporária do indivíduo à época dos fatos.

Porém, outros projetos de lei, que abarcam de modo mais amplo, as diversas situações, encontram-se em debate na Câmara Legislativa, como é o caso do PL 10.860/2018, que busca incorporar o direito ao esquecimento, como elemento constituído dos direitos da personalidade, resguardado no âmbito constitucional.

3.3 - Projeto de Lei 10.860/2018 – direito ao esquecimento – princípio da dignidade da pessoa humana – direitos da personalidade

O Projeto de Lei 10.860/2018, de autoria do Dep. Augusto Carvalho - SD/DF, visa instituir o direito ao esquecimento no códex civil brasileiro, trazendo-o como um dos direitos da personalidade: "EMENTA: Acrescenta parágrafo único ao art. 11 da Lei nº

10.406, de 10 de janeiro de 2002, que institui o Código Civil, instituindo o direito ao esquecimento" (BRASIL, 2018).

Nota-se que o autor do referido projeto busca acrescentar aos direitos da personalidade o direito ao esquecimento, balizando-se, em especial, no princípio da dignidade da pessoa humana. Entretanto, o projeto está parado na Comissão de constituição e justiça da casa legislativa desde fevereiro de 2019.

De toda a sorte, conforme se observa, há inúmeras iniciativas no âmbito do legislativo brasileiro, buscando amparar de forma taxativa, esse direito, mas que encontra resistência, por falta de apoio político e pressão social.

Considerações Finais

Diante de todo o exposto, verifica-se que o Estado brasileiro caminha a passos largos na positivação explícita do direito ao esquecimento, notadamente, no meio digital, enquanto direito e garantia fundamental, não sendo, portanto, razoável dizer que no cenário brasileiro, a novel LGPD tenha recepcionado o Direito ao Esquecimento.

É certo que a LGPD foi inspirada no RGPD em vários pontos, principalmente no tocante a sua base principiológica, mas isso não significa dizer que a LGPD é uma reprodução exata do RGPD. Por várias razões, que seria necessário um outro artigo para discorrer sobre, a LGPD, diferentemente do RGPD, deixou um considerável número de dispositivos que carecem de normatização a cargo da Autoridade Nacional de Proteção de Dados – ANPD, a qual já vem normatizando muitos desses dispositivos.

De fato, percebe-se claramente que o legislador nacional optou, em determinados aspectos não seguir a similaridade construída entre os dois normativos e é exatamente o que ocorre com a hipótese relativa ao Direito à Eliminação, que não adotou a expressão Direito ao Apagamento do modelo europeu.

E é sobre essa perspectiva, que é perceptível não ser possível se extrair da LGPD qualquer correlação entre o Direito à Eliminação e o Direito ao esquecimento. O que se verifica, até mesmo, pela análise dos casos concretos apresentados, é que prevalece o entendimento de que o Direito ao Esquecimento está relacionado à perda do interesse público que ao longo do tempo, determinadas informações deixam de ter relevância ou importância.

No Brasil, nota-se que o conflito existente sobre o Direito ao Esquecimento está, predominantemente, centrada no modelo estrutural tradicional, que envolve o equilíbrio entre o direito à privacidade e o direito à informação. Em outras palavras, esse conflito ocorre em meio ao embate entre o interesse individual na preservação da privacidade e o interesse coletivo na liberdade de informação e tudo isso sob a ótica da subsistência do interesse público, modulado pelo princípio constitucional da Dignidade Humana.

Em síntese, percebe-se que o conflito no cenário brasileiro sobre o Direito ao Esquecimento está inserido em um contexto complexo, onde a ponderação entre direitos individuais e coletivos, a subsistência do interesse público e o respeito à dignidade humana são elementos centrais na construção de decisões judiciais e políticas públicas relacionadas a esse tema.

Desta feita, evidencia-se e reforça o entendimento de que a LGPD, por si só não conseguiria esgotar este conflito, dada a sua impossibilidade de correlação com o Direito ao Esquecimento. A legislação representa um grandioso passo na construção da proteção e privacidade de informações pessoais, inclusive, em meios digitais e enfrenta consideráveis desafios na sua implementação que está muito ligada a uma verdadeira mudança cultural, mas que já tem trazido resultados significativos.

Portanto, uma possível solução é o poder público e a sociedade organizada, criarem mecanismos dinâmicos para a solução dessa espécie de conflito, para que sejam resolvidos de maneira eficaz e dinâmica, e quem sabe pautar o Direito ao Esquecimento como regra e não exceção. Envolver a Autoridade Nacional de Proteção de Dados – ANPD na discussão do Direito ao Esquecimento, também pode ser fundamental para as mudanças que se entende necessárias e, mais ainda, quem sabe até avaliar ajustes na LGPD de modo que possa abordar questões específicas relacionadas ao Direito ao Esquecimento.

Referências bibliográficas

ADAMS, John. Risco. Tradução de Lenita Rimou Esteves. São Paulo: Senso, 2009. p. 250-251.

BARRETO, Vicente D. P. O fetiche dos direitos humanos e outros temas. Rio de Janeiro: Lúmen Juris, 2010.

BAUMAN, Zygmunt. Modernidade Liquida. Rio de Janeiro: Jorge Zahar, 2001.

BECK, Ulrich. Sociedade do Risco – Rumo a uma outra modernidade. São Paulo: editora 34. 2011.

BRASIL. Câmara dos Deputados. Projeto de Lei 10.860/2018, 2018. Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2184113. Acesso em: 18 fev. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 fev. 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei 4306/2020, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2260784. Acesso em: 15 fev. 2021.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988, Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 nov. 2020.

CASTELLS, Manuel. A Sociedade em Rede – A Era da Informação: Economia, Sociedade e Cultura. São Paulo: Paz e Terra, v. VI, 1999.

DONEDA, Danilo. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Brasília: SDE/DPDC, 2010.

FORTINE, Cristiana; ESTEVES, Júlio C. D. S.; DIAS, Maria F. T. Políticas Públicas. Belo Horizonte: Editora Fórum, 2008.

FOUCAULT, Michel. Vigiar e Punir: nascimento da prisão. Tradução de Lígia M. Ponde Vassalo. Petrópoles: Vozes, 1987.

GIDDENS, Anthony. As conseqüências da modernidade. Tradução de Raul Fiker. São Paulo: UNESP, 1991.

LENZA, Pedro. Direito Constitucional esquematizado. 24. ed. São Paulo: Saraiva Educação, 2020.

LUHMANN, Niklas. Sociologia del Riesgo. Tradução de Silvia Pape; Erker Brunhilde, et al. 1ª. ed. Guadalajara: Universidad Iberoamericana, 1992.

SCHOMBERGER, Viktor M. Delete – The Virtue of Forgetting in the Digital Ace, 2009. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=ZrqvYOBm_sMC&oi=fnd&pg=PP1&dq=viktor+mayer+sch%C3%B6nberger+&ots=6p9tU1CSaP&sig=saXFyUAHEUxTXRCGs58Xvg_xPuk#v=onepage&q&f=false. Acesso em: 05 fev. 2021.

STF. Voto do Relator Min. Dias Toffoli. RE n. 1.010.606: Rel. Min. Dias Toffoli, 2021. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/RE1010606VOTOMDT.pdf. Acesso em: 02 mar. 2021.

STJ. 4ª Turma. REsp n. 1.334.097 – RJ: Rel. Min. Luis Felipe Salomão, 2013. Disponível em: https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj.pdf. Acesso em: 02 mar. 2021.

TJ-DF. Acórdão n. 971472, Relator Juiz Aiston Henrique de Sousa, 2ª Turma, Data de Julgamento: 5/10/2016, publicado no DJe: 13/10/2016. JusBrasil, 2016. Disponível em: https://tj-df.jusbrasil.com.br/jurisprudencia/913949605/7292924720158070016-segredo-de-justica-0729292-4720158070016. Acesso em: 21 nov. 2020.

TJ-SC. Apelação Cível: 03245282520148240023 Capital 0324528-25.2014.8.24.0023, Relator: José Agenor de Aragão, Data de Julgamento: 19/09/2019, Quarta Câmara de Direito Civil. JusBrasil, 2019. Disponível em: https://tj-sc.jusbrasil.com.br/jurisprudencia/759601613/apelacao-civel-ac-32452825201482400 23-capital-0324528-2520148240023. Acesso em: 27 nov. 2020.

TRATADO Internacional - Convenção Americana de Direitos Humanos - Pacto de São José da Costa Rica. Site da Procuradoria Geral do Estado de São Paulo, 22 Novembro 1969. Disponível em: http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm. Acesso em: 03 Setembro 2020 às 12:35.

UNIÃO EUROPÉIA. Regulamento Geral sobre a Proteção de Dados. Artigo 17 - Direito ao apagamento dos dados («direito a ser esquecido»), 22 maio 2020. Disponível em: https://gdpr.algolia.com/pt/gdpr-article-17. Acesso em: 17 nov. 2020.

Digital Constitutionalism and Internet's Regulation – New Challenges

Diana Camões[355]

Abstract

The Internet has created several challenges in our daily life. Being considered the new public forum, it has become a crucial place for individuals to exercise their fundamental rights. This essay reflects about the consequences of the Internet's regulation and it analyses two different scenarios: countries where there has been the development of digital authoritarianism and western democracies, where private actors play a crucial role and are able, without any intervention, to restrict freedom of expression and disrespect data protection law. With the advent of social media, this has become more critical. After all is it possible to find a balance between these different interests? How can we protect individuals from arbitrary interventions? On the other hand, how does the Internet regulation affect the democratic principle? These are some of the questions answered in this essay, adding a special reflection about the importance of digital constitutionalism nowadays to face these challenges.

Key words: digital constitutionalism; internet; fundamental rights; democracy; data protection law.

[355] Licenciada em Direito pela Faculdade de Direito da Universidade Católica (Escola do Porto), Mestranda em Direito Internacional e Europeu pela Faculdade de Direito da Universidade Católica (Escola do Porto) e Pós-Graduanda em Direito da Proteção de Dados pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa.

Email: diana.camoes@hotmail.com

Digital Constitutionalism and Internet's Regulation – New Challenges

Diana Camões

Resumo
A Internet criou vários desafios no nosso quotidiano. Sendo considerada o novo fórum público, tornou-se num espaço crucial para os indivíduos exercerem os seus direitos fundamentais. Este artigo reflete sobre as consequências da Regulação da Internet e analisa dois cenários diferentes: países onde houve o desenvolvimento do autoritarismo digital e as democracias ocidentais, onde os atores privados desempenham um papel crucial e conseguem, sem qualquer intervenção, restringir a liberdade de expressão e desrespeitar o direito da proteção de dados. Com o advento das redes sociais, isto tornou-se mais crítico. Afinal, é possível encontrar um equilíbrio entre estes interesses distintos? Como poderemos proteger os indivíduos de intervenções arbitrárias? Por outro lado, como é que a Regulação da Internet afeta o princípio democrático? Estas são algumas das questões respondidas neste artigo, adicionando-se uma especial reflexão sobre a importância do constitucionalismo digital para enfrentar estes desafios.

Palavras-Chave: constitucionalismo digital; internet; direitos fundamentais; democracia; direito da proteção de dados.

Acronyms and Abbreviations

Berkeley Tech.L.J.	Berkeley Technology Law Journal
CJEU	Court of Justice of the European Union
Charter	Charter of Fundamental Rights of the European Union
ECHR	European Convention on Human Rights
EctHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
UN	United Nations
UNC	United Nations Charter
US	United States Supreme Court
Wash. U. L. Rev	Washington University Global Studies Law Review

1. Introduction

The Internet changed the way how we perceive the world. Through the new technologies, the quality of our life improved and new challenges arose. Nowadays, it's impossible to live without the digital world and, in fact, this has created new dynamics of the citizens' fundamental rights.[356] Not only the private sector has an important influence, but also the illiberal regimes may use it as a tool to "bring forward novel concerns about embedding control and surveillance in global technologies, at a time of growing technological polarization."[357] Therefore, constitutionalism itself cannot be indifferent to those changes, especially with this new "global constitutional order"[358] [359], where power is "shared between national and supranational rulers"[360] that are supposed to ensure the fulfillment of fundamental rights at different levels.[361]

---

[356] Luciano Floridi, "The Fight for Digital Sovereignty: What it is, and why it matters, especially for the EU" *Philosophy & Technology*, v. 33 (2020):369, Accessed 2 November, 2022, < https://link.springer.com/article/10.1007/s13347-020-00423-6 > talks about the importance of digital sovereignty and how "the states have the power to regulate the digital, and this is a powerful form of cybernetic control, exercised by determining what is legal or not."

[357] Giovanni de Gregorio and Roxana Radu, "Digital Constitutionalism in the new era of internet governance", *International Journal of Law and Information Technology*, v. 30, no. 1 (2022): 68-69.

[358] David Schneiderman, "A New Constitutional Order", in *Research Handbook on Comparative Constitutional Law,* ed. Rosalind Dixon, Tom Ginsburd (Edward Elgar Publishing, 2011), 189.

[359] Three features are distinct in understanding transnational constitutionalism, mainly the development of transnational constitutions or quasi-constitutional arrangements, the abundance of transnational judicial dialogues and the global convergence of national constitutions. See Jiunn Yeh and Wen-Chen Chang, "The Emergence of Transnational Constitutionalism: Its features, Challenges and Solutions", *Penn State Law Review*, v. 27, no. 1 (2008):89.

[360] Catarina Santos Botelho, "Transnational Constitutional Law", in *Max Planck Encyclopedia of Comparative Constitutional Law*, ed. Grote, R., Lachenmann,F, and Wolfrum, R, (eds) (Oxford: Oxford University Press, 2020), forthcoming at https://oxcon.ouplaw.com/

[361] At a universal scale, we should mention the UN, being mostly important the UNC. Bardo Fassbender, "The United Nations Charter as the Constitution of the International Community", *Columbia Journal of International Law*, v. 36, no. 3 (1998): 529 considers that this is the "world order constitution". On the contrary, Anne Petters, Transnational Law comprises Constitutional, Criminal and Quasi-Private Law, in *Making Transnational Law work in the global economy,* ed. Pieter Bekker et al., (Cambridge: Cambridge University, 2010):164 states the UCN "is not the world constitution" and that "the absence of a constitutional document means that the international constitutional law cannot be easily identified through formal criteria". Neil Walker, "Constitutionalism and Pluralism in Global Context" in *Constitutional Pluralism in the European Union and Beyond,* eds Matej Avbelj, Jan Komárek (Oxford: Hart Publishing, 2012): 26 also alerts for the fact that this is "far from suggesting a world state to subsume and replace the category of nation state". As B. Ramcharan, *The Concept and Present Status of the International Protection of Human Rights – Forty years after the Universal Declaration* (Leiden: Nijhoff Publishers, 1989): 268, reminds we cannot forget that, at a universal level, that "commitment is frequently lacking" and, consequentially, the international community "often finds itself unable to act on the protection of human rights."

After all, which citizens' rights are at stake? Is it possible to control Internet and still respect the democratic principle? How can constitutionalism face this challenge? These are some of the questions that I'll try to answer with this essay.

2. The internet Law

The Internet Law is one of the most recent branches of the Law, whose existence is inevitable nowadays and it can be defined as "the field of law where the Internet plays a central role in the legal analysis."[362] It's a "network of networks"[363], as if it was a real place where people from all around the world use different websites, social media and other tools.

This is, however, the side of the internet[364] that is accessible to everyone. Beneath this "side" also exists the dark web, a "space that is rarely visited, highly encrypted and seldom regulated."[365] Over the years, its development led to new legal issues, regarding intellectual property law, robotics, cybercrimes, commerce and data protection law. Even though, as we'll see, the states have a huge impact in this regulation, we should remember the impact of non-state actors, mainly due to "the development of certain Internet spaces which are primarily governed by rules laid down by service providers."[366]

3. Which fundamental rights are at risk?

The Liberal movements allowed the recognition of certain rights attributed not to all people, but only to a minority, namely "the bourgeois elite."[367] Nowadays, the fundamental rights are attributed to everyone, irrespective of the gender, race, age or class. Freedom of expression is one of the rights that arises many doubts, mainly in

---

[362] Arno Lodder, "Internet Law: A Brief Introduction", *SAGE Encyclopedia of the Internet,* in ed. Barney-Warf (2018) <https://ssrn.com/abstract=3191751> accessed 25 October 2022.

[363] Michael Rustad, *Global Internet Law* (Third Edn, West Academic Publishing, 2020), 2.

[364] Derrick Cogburn, "The Multiple Logics of Post-Snowden Restructuring of Internet Governance" in FRANCESCA MUSIANI et al (eds) *The Turn To Infrastructure in Internet Governance* (Palgrave Macmillan, 2016) 25, 30, says that there are three "functional areas" to global internet governance, such as the technical standardization, the resource allocation and assignment and, finally, the policymaking.

[365] Andres Guadamuz, "Internet Regulation" in Lilian Edwards (ed), *Policy and The Internet Law* (Hart Publishing, 2018) 3, 5. Most of the world's population doesn't have the means to access the Dark Web.

[366] Pedro Asensio, *Conflict of Laws and The Internet* (Edwards Elgar Publishing, 2020) 4.

[367] Joan Mir and Marco Bassini, "Freedom of Expression in the Internet" in *The Internet and Constitutional Law – The Protection of Fundamental Rights and Constitutional Adjudication in Europe,* eds. Oreste Pollicino and Graziella Romeo (Abingdon: Routledge, 2016), 72.

order to know if the restrictions created in the online world are lawful.[368] This new era of "decentralization of communications and culture" led to "new opportunities for any individual to receive content, and to speak as well in the online world."[369] Article 10 of the ECHR assures that "everyone has the right to freedom of expression." Of course, that this isn't an absolute right, because in certain circumstances allows for derogations[370] (10º/2).[371] Therefore, Article 10 is not intended "to act as an umbrella for shielding citizens from speech they might find unpleasant, offensive or merely rude, according to their own subjective views and experiences."[372] On the other hand, Article 11º of the Charter of Fundamental Rights of the European Union (Charter) states that "everyone has the right to freedom of expression", including without apparent restraints "freedom to hold opinions and to receive and impart information and ideas." It's now important to see how the ECtHR has analyzed over the years the exercise of this right in the internet. One of the leading cases related to freedom of expression in the internet is the *Ahmet Yildirim v. Turkey*.[373]

In this case, the applicant owned and ran a website on which he published his academic work. However, he was unable to access his site, because there was an order to block all access to Google Sites as a preventative measure in criminal proceedings. Nevertheless, the ECtHR considered that not only there wasn't a legal framework to regulate the scope of the ban as well as "the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information."[374] [375] There was, therefore, an important recognition that "Article 10 includes a right of internet access"[376] Second, in the *Cengiz and Others v.*

---

[368] *Ibid.* Initially, freedom of expression was "understood in the sense of absence of interference" by the state. It was the "massification" operated by the media that led to a different approach of freedom of expression.

[369] *Ibid,* 81.

[370] The restrictions must be (i) prescribed by law, (ii) have a legitim aim and (iii) be necessary in a democratic society. We won't be able to see everything regarding this topic.

[371] As Frederick Schauer, "Freedom of Expression Adjudication" in George Nolte (Ed.) *European and US Constitutionalism* (Cambridge University Press, 2005), 49, 52-53, says this type of protection "explicitly authorizes a process of balancing the interest in freedom of communication against other countervailing interests."

[372] Adina Portaru, Freedom of Expression Online – The Code of Conduct on Countering Illegal Hate Speech Online" (2017) 4 Romanian Review of European Law 77, 82.

[373] *Ahmet Yildirim v Turkey* Application number 3111/10 (ECtHR, 18 December 2012).

[374] *Ibid,* Paragraph 54.

[375] As Mir and Bassini (n 12), 83 say this case established "for the first-time detailed conditions and restrictions that would apply to any attempt to restrict access to internet content."

[376] Jacob Rowbottom, "The Protection of Expression in the UK" in Oreste Pollicino and Graziella Romeo (Eds) *The Internet and Constitutional Law – The Protection of Fundamental Rights and Constitutional Adjudication in* Europe (Routledge, 2016) 192, 206.

Turkey[377] case, regarding blocking of access to *Youtube,* the ECtHR held that this decision affected the applicant's right "to receive and impart information and ideas" in which Article 10 "guarantees not only the right to impart information, but also the right of the public to receive it."[378] More recently, in *Vladimir Kharitonov v. Russia*[379], the ECtHR stated that there was a breach of Article 10, due to the blocking of different websites. Once again, the court defended the importance of the internet as a tool in the exercise of freedom of expression.[380] As some of these cases demonstrate, this "constitutes an essential basis of a democratic society" and "limitations on that freedom are interpreted strictly."[381] However, the ECtHR has already stated that the internet is "likely to raise new problems for the protection of fundamental rights and that the measures applied to traditional media will not work effectively in the new digital environment."[382]

It's now interesting to briefly analyze, from a comparative constitutional law point[383] of view, the USA's system. The *First Amendment* consecrates freedom of

---

[377] *Cengiz and Others v. Turkey*, Application 48226/10 and 14027/11 (ECtHR, 1 December 2015).

[378] *Ibid,* Paragraphs 55 and 56.

[379] *Vladimir Kharitonov v. Russia* Application 10795/14 (ECtHR, 23 June 2020). On the contrary, in the *Delfi AS v. Estonia* Application number 64569/09 (ECtHR, 10 October 2013) the ECtHR held that the restriction on the freedom of expression was justified and proportionated.

[380] There was a violation of Article 13, taken in conjunction with article 10, because "the Russian courts had not considered the substance of his grievance relating to the blocking of access to the applicant's website."

[381] European Court of Human Rights, Guide to the Case-Law of the European Court of Human Rights Data Protection (ECtHR, 2022), 17. Regarding the press, the ECtHR states that "national authorities must be careful to respect the duty of journalists do disseminate information on questions of general interest, even if they have resource to a degree of exaggeration or provocation."

[382] Oreste Pollicino and Graziella Romeo, "Internet Law, Protection of Fundamental Rights and the role of Constitutional Adjudication" in Oreste Pollicino and Graziella Romeo (eds) *The Internet and Constitutional Law – The Protection Fundamental Rights and Constitutional Adjudication in Europe* (Routledge, 2016), 240.

[383] Regarding the advantages and disadvantages of constitutional comparison see Catarina Botelho, "Comparative Constitutional Studies 2.0 – Lost in Translations Revisited" in Rita Lobo Xavier et al (Ed) *Constitucionalismos e (con)temporaneidade Estudos em Homenagem ao Prof. Doutor Manuel Afonso Vaz* (Universidade Católica Editora, 2020, Porto), 33-37. Nevertheless, it's interesting to see how the PCC has approached this question. As CATARINA BOTELHO, "Is There a Middle Ground Between Constitutional Patriotism and Constitutional Cosmopolitanism? The Portuguese Constitutional Court and the Use of Foreign (Case) Law" in Giuseppe Franco Ferrari (Ed.), *Judicial Cosmopolitanism - The Use of Foreign Law in Contemporary Constitutional Systems* (Brill Nijhoff, 2019), 446-448, points out "in the Portuguese case, it is fair to conclude that more than a comparative constitutional law approach, we have reputable comparative constitutional jurisprudence approach. This is not surprising, since the Portuguese History Has been highly influenced by multiple connections with other nations."

expression as an absolute right[384], stating that the "congress shall make no law abridging the freedom of speech or of the press."[385] One of the most interesting cases is *LICRA v. Yahoo*. LICRA filed a civil complaint against Yahoo, a US service provider, due to the fact that this platform allowed the sale of Nazi Memorabilia, in violation of the French Criminal Code.[386] Consequentially, the Court ordered Yahoo to take all measures to eliminate access to Nazi memorabilia. Nevertheless, Yahoo didn't fulfill that order because it didn't recognize jurisdiction for the French Court and thought that there was a violation of freedom of expression, under the First Amendment. This case is special because, as MARC GREENBERG points out, it shows "how far we have to go in resolving how jurisdictional principles do or should work on the international Internet and illustrates the importance of addressing these issues as a global community."[387] [388]

The US Supreme Court has considered that freedom of speech includes the right not to speak,[389] the right to use fighting words to spread political messages[390] or even to contribute with money for political campaigns.[391]

The first Amendment doesn't, however, cover threats[392], solicitations to engage in illegal activities[393] and even promoting the use of illegal drugs in a school.[394]

---

[384] According to Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart Publishing 2021) p. 42, one of the reasons for this difference is the fact that the "US First Amendment is the sole and sacred point of reference".

[385] As Frederick Schauer (n 16) 52, says, due to "incorporation of the First Amendment by the Fourteenth Amendment, the First Amendment delimits the powers of the states as well as those of the federal government."

[386] More precisely Article R645/1.

[387] Marc Greenber, "A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market" (2003) 18 Berkeley Technology Law Journal (Berkeley Tech.L.J.) 1191, 1199.

[388] Oreste Pollicino and Marco Bassini, "The Law of The Internet: Between Globalization and Localization" in Miguel Poiares Maduro *et al* (Ed) *Transnational Law – Rethinking European Law and Legal Thinking* (Cambridge University Press, 2014), 366, affirm that this case shows "why this dialogue is still troublesome today" due to the "differences between values and the connected degree of protection under national constitutions." The authors say that this also demonstrates how there are "problems in enforcing judgments issued by foreign courts."

[389] Or more precisely, not to salute the flag. See *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943).

[390] Cohen v. California, 403 U.S. 15 (1971). Cohen, in this case, was accused of disturbing the peace for wearing a jacket that said "Fuck the Draft" in a courthouse.

[391] Buckley v. Valeo, 424 U.S. 1 (1976).

[392] See Virginia v. Black, 538 U.S. 343 (2003).

[393] United States v. Williams, 553 U.S. 285 (2008)

[394] Morse v. Frederick, 551 U.S. 393 (2007).

It's also interesting to see how the US Court of Justice has adapted these considerations into the online world. ORESTE POLLICINO states that the "US Supreme Court has transposed the offline balancing of fundamental rights into the online domain."[395] Nevertheless, as we've seen, the First Amendment doesn't allow the existence of government's restrictions, which makes us think how "private actors may be more restrictive than government actors"[396], which means that "speech that cannot be prohibited by the state under the first amendment can be prohibited by private platforms online."[397] This demonstrates that the protection of these rights doesn't fall only within the scope of the government. The online dimension strengthened the platforms' powers, because most times, the users are limited by the company's rules. ORESTE POLLICINO considers that "the advent of the internet has resulted in a further enhancement of the already vast protection enjoyed by freedom of speech in the world of atoms."[398] As an example, in *Packingham v. North Carolina*[399], The US Court of Justice held that "one of the most important places to exchange views is cyberspace, particularly social media", concluding that the North Carolina violated the First Amendment[400] when it prohibited registered sex offenders from using social media. This's a clear example of how freedom of speech is seen in the USA.

As I had the chance to mention before, the Internet may also have a huge impact on the citizens' privacy. Regarding this topic, Article 8 of ECHR consecrates *the right to privacy*[401], which is also foreseen in Article 7 of Charter. Nowadays, within the EU context, there has been a huge attempt to protect personal data, being most important the General Data Protection Regulation (GDPR).[402] Within this context,

---

[395] Oreste Pollicino, *nº 30,* 58-59. For an approach of the first amendment protection for search engine search results, see Eugene Volokh, "First Amendment Protection for Search Engine Search Results" (2012) 12(22) *UCLA School of Law Research Paper* 1, 3-27.

[396] Claudia Haupt, Regulating Speech Online: Free Speech Values in Constitutional Frames" (2021) 99 Nbr 2 Wash. U. L. Rev. 751, 768.

[397] *ibid,* 768-769.

[398] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* 67.

[399] Packingham v. North Carolina, 582 US, (2017).

[400] As the Court says, "convicted criminals—might receive legitimate benefits from these means for access to the world of ideas, in particular if they seek to reform and to pursue lawful and rewarding lives."

[401] The 1976 Portuguese Constitution was the first to assure a right to informative self-determination (Art. 35º). Alexandre Pinheiro, *Privacy e Proteção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional* (AAFDL, 1st edn, 2015) 777, considers that the data protection must be integrated in a right of higher latitude, maxime the *right to informational identity*.

[402] Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and

technology (internet) may be used as a tool to control citizens. In *Roman Zakharov v. Russia*[403], the ECtHR held that:

"The domestic legal provisions governing the interception of communications did not provide adequate and effective guarantees against arbitrariness and the risk of abuse. The domestic law did not meet the quality of law requirement and was incapable of keeping the interference to what was necessary in a democratic society."[404]

Regarding this topic, the Case *Digital Rights Ireland*[405] assumes an important role, as Alexandre Pereira points out.[406] [407] After briefly presenting some of the fundamental rights that may be affected, it's now time to analyze how the internet may be regulated.

4. Internet's Regulation: The Fight for Digital Sovereignty? How does that affect the democratic principle?

The Internet's regulation isn't an easy topic to discuss. As ELBERT LIN says, "the internet is the largest computer database ever, with a nearly memory and access to arguably the largest possible stream of information."[408] Having this in mind, the way how the Internet is treated may be an indicative factor of a political system's evaluation. Furthermore, a distinction must be done in accordance with the following situations: *(i)* States that censorship the Internet, *(ii)* States that, even though respect the

---

on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). It's important to mention that this wasn't the first time that there was concern to regulate this. Actually, the first law to emerge about data protection law was Hessisches Datenshutzgesetz, in Germany, the Datalog, in 1973 (Sweden) and the Privacy Act (1974). Despite that, from an historical point of view, it was firstly in the USA that there was a huge discussion, in 1960, in the special subcommittee on invasion of privacy.

[403] *Roman Zakharov v. Russia* Application number 47143/06 (ECtHR 4 December 2015)

[404] See also *Big Brother Watch and Others v. United Kingdom*, Application number 58170/13, 62322/14 and 24960/15, (ECtHR 25 may 2011) *and Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application number. 62540/00 (ECtHR 28 June 2007), paragraph 93.

[405] *Digital Rights Ireland Ltd* (C-293/12) 8 April 2014.

[406] Alexandre Pereira, "Direito ao respeito pela vida privada digital" in Paulo Pinto de Albuquerque (Ed) *Comentário da Convenção Europeia dos Direito Humanos e dos Protocolos Adicionais – Volume II* (Universidade Católica Editora, 2019) 1451, 1462-1466.

[407] After all, "those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them" (paragraph 47, nº 51).

[408] Elbert Lin, "Prioritizing Privacy: A Constitutional Response to the Internet" (2002) 17 Number 3 Berkeley Tech.L.J 1085, 1106-1107.

democratic principle, share "powers" with the Private Actors. One thing is clear: nowadays, it isn't possible to defend a "cyber-libertarian" vision, mainly due to the fact that "cyberspace has experienced, when state eagerly cooperated with the giants of digital technologies to disseminate and legitimize their ideas and tolls for control."[409]

Firstly, many countries around the world create huge restrictions, in order to prevent their citizens from accessing the Internet freely. Their main goal is to create a domestic internet, which contributes for the state's isolation. As an example, it's important to mention Iran. In 2019, they announced that its intranet was almost ready to shield Iran from harmful internet.

The Iranian Parliament is moving to ratify the *User Protection Bill,* whose main goal will be to block foreign websites and platforms "run by foreign companies still operating in Iran, require people to use IDs to access the internet and criminalize the distribution and sale of Virtual Private Networks (VPNs). It will also require social media platforms to cooperate with the Government in surveillance and censorship."[410] This will allow Iranian citizens to be even more isolated[411], whose lives are at stake with the recent uprisings. The UN and Human Rights Organizations have stated that this constitutes a violation of fundamental rights. With the most recent protests that have spread around the Country, the government decided to block access to online platforms, such as Instagram, WhatsApp, in order to stop the protests, which didn't work as we all know.[412]

Another example is Russia. Putin's regime took a step towards internet isolation, with the creation of its sovereign internet project: RuNet.[413] As JUSTIN SHERMAN points out, "the Kremlin is pursuing internet isolation on a fundamentally deeper level than

---

[409] Marwa Azelmat, "The rise of digital authoritarianism: is the internet to be Blamed" (European Master's Degree in Human Rights and Democratisation, Queen's University of Belfast, 2019) 44.

[410] United Nations "Human Rights UN human rights experts urge Iran to abandon restrictive internet bill", (1 march 2022) <https://www.ohchr.org/en/press-releases/2022/03/un-human-rights-experts-urge-iran-abandon-restrictive-internet-bill> accessed 20 October 2022.

[411] And the LGBTQI community is likely to be targeted even more with this reform. Sayeh Isfahani, "The Internet Protection Bill will hurt all Iranians, but the queer community will have the most to lose" (*Atlantic Council* 12 April 2022) <https://www.atlanticcouncil.org/blogs/iransource/the-internet-protection-bill-will-hurt-all-iranians-but-the-queer-community-will-have-the-most-to-lose/> accessed 15 October 2022, calls attention for the fact that "several key provisions in the Protection Bill pose an imminent threat to freedom of expression in Iran and endangers the LGBTQI community in particular."

[412] Weronika Strzyżyńska "Iran blocks capital's internet access as Amini protests grow" *The Guardian,* 2022 (London, 22 September 2022).

[413] This was always a goal for Russia. However, in 2019, they took a step forward with the discussion of the Bill in the Duma. The reform ended up being approved, as it was expected.

many other countries."[414] This raises many concerns, not only for Russian citizens, but also to the other states.[415] However, the regime is taking this to another level, due to the "intimidation, harassment by security services, court-ordered fines, and complex, restrictive, and inconsistently enforced speech laws."[416]

One of the main reasons invoked for this strategy is the "perception of a US-posed cyber threat"[417]. After the Invasion in Ukraine, many rumors arose regarding the country's intent to cut itself off from Global Internet.[418] This led to the ban of Facebook and Instagram, due to the fact the Court in Moscow considered that the Meta Group was "carrying out extremist activities."[419] There was, however, a concern that the imposition of sanctions would increase "the disrupt internet access in Russia and Belarus."[420] This statement points out an important thing: isolating the access even further is not the answer, especially having in mind that the citizens don't have already the means to be aware of the facts and spread their ideas and thoughts.

Finally, one of the main concerns is China. Over the years, the Communist Party has increased its control over the internet, which got worse after Covid'19. The Freedom House points out that there has been a continuous attempt to block mobile apps and prosecute who provides access to them.

On the other hand, the government passed rules and new laws in order to regulate how the personal data is collected, which allows for a bigger control over citizens privacy and exercise of rights. For these reasons, in 2021, China was considered a Not Free with a score of 10/100 (scale of 0 – least free- to 100 – most

---

414 Justin Sherman, "Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior" (*The Atlantic Council,* 12 July 2021) < https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/> accessed 14 October 2022, p. 2.

415 Let's just keep in mind what happened in the 2016 Presidency Election, in the USA.

416 Justin Sherman, nº 59, 4.

417 *ibid,* p. 5.

418 Bhaswati Guha Majumder, "Russia Could Cut Itself off from Global Internet by March 11: New Documents show" *News 18* (9 march 2022)

419 Pjotr Sauer, "Russia Bans Facebook and Instagram under extremism law" *The Guardian* (London, 21 March 2022).

420 Regarding this problem, there was a Joint Statement made by the Civil Society calling attention that cutting Internet services in Russia would be counterproductive, because "people would find even harder to find accurate news, and the internet, for all its faults, remains the last open space for free-flowing discourse." Freedom House, "Civil society to U.S. government: Do not disrupt internet access in Russia or Belarus" (Freedom House, 10 March 2022) <https://freedomhouse.org/article/civil-society-us-government-do-not-disrupt-internet-access-russia-or-belarus> accessed 24 October 2022.

free).[421] This is why China is considered to be the country "whose online censorship is causing the greatest damage – on individual as well as commercial freedom."[422] After all, the *Great Firewall of China* (a system that allows the government to intercept internet traffic and block connections to websites and servers that mustn't be acceptable), implemented in the 90's has shown its efficiency and it was "more or less matched by few countries).[423] It's considered to be "The Golden Shield."[424]

These examples clearly show how the Internet's regulation affects the democratic principle.[425] In fact, the doctrine talks about *digital authoritarianism*[426], which represents "the use of technology by authoritarian governments not only to control, but to shape the behavior of its citizens via surveillance, repression, manipulation, censorship and expand political control."[427] We can also define it as "the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control and/or undermine civil liberties."[428]

There is, nevertheless, a paradox, because the digital world "enables efficient state control and coercion of citizens" but it also "reduces the necessity to resort to

---

[421] Freedom House "Concerns demonstrated by the Freedom House" (*Freedom House,* 2021*)* <https://freedomhouse.org/country/china/freedom-net/2021> accessed 24 October 2022.

[422] Erixon Frederik and Hosuk Lee-Makiyama, "Digital Authoritarianism: Human Rights, Geopolitics and commerce" (2011) 5/2011 EUROPEAN Center for International Political Economy <https://www.econstor.eu/bitstream/10419/174715/1/ecipe-op-2011-5.pdf> accessed 25 October 2022, 5.

[423] Claudiu Codreanu, "Using and Exporting Digital Authoritarianism: Challenging both cyberspace and democracies" (2022) 16 1 *Europolity* 39, 43.

[424] Erixon Fredrik and Hosuk Lee-Makiyama, nº 67, p. 5.

[425] The examples mentioned aren't the only ones. As Michael Rustad, nº 8, p. 74, points out "two-thirds of all Internet Users – 67% - live in countries where criticism of the government, military, or ruling family is subject to censorship (…) The Report Found that only a quarter (24%) of the internet's population had completely free access."

[426] Cladiu Codreanu, nº 68, 43-44 calls attention for the three generations of digital authoritarianism proposed by Ron Deibert: (1) the first phase led to the creation of borders in the cyber space in order to restrict citizens' rights, (2) phase of consolidation of information through laws and regulations and (3) phase of targeted espionage, surveillance and disruptions in cyberspace.

[427] Lydia Khalil, "Digital Authoritarianism, China and COVID" (*Institute for International Policy,* 2020) <https://www.lowyinstitute.org/sites/default/files/Khalil%2C%20Digital%20Authoritarianism%2C%20China%20and%20Covid_web_print_021120.pdf> accessed 24 October 2022, 6

[428] Erol Yaboke, "Promote and Build a Strategic Approach to Digital Authoritarianism" (*Center for Strategic International Studies,* October 2020) <https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism > Accessed 24 October 2022, 1.

coercion at all."[429] However, even if those countries try to isolate themselves from the rest of the world, they still may pose a threat, especially to the western democracies.[430] One of the problems regarding this matter, for example, is Artificial Intelligence, because it "tends to empower centralized autocratic government rather than decentralized democratic governance"[431] and China is, at the moment, one of the major "supplier and driver of AI surveillance technologies."[432] We must take into account that China is selling these technologies to countries less developed (and even western countries), which is allowing the exportation of "its version of authoritarianism."[433] On the other hand, these technologies may also be used as a tool against the western democracies. Over the years, we've seen several attempts to finance some parties in Europe. Since 2014, Russia has secretly funneled at least 300 million dollars to foreign political parties and candidates in more than two dozen countries.[434]

The main goal would be the increase of its influence in several countries across the globe. However, this isn't new. After the Brexit Referendum, several concerns were raised with the possibility of Russia's influence in it, with British Ministers being accused of turning "a blind eye to possible interference by Moscow" and Russia's influence has been interpreted as "the new normal"[435], which might change with the on-going conflict. Additionally, the 2016 US presidential election was apparently influenced by Russia.

Consequentially, the Senate Intel Committee's bipartisan report on Russia's Use of social media confirmed that Russia aimed helping to put Donald Trump in the Oval office, stating that this was "part of a broader, sophisticated and ongoing information

---

[429] Lydia Khalil, nº 72, p. 7.

[430] For a deeper analysis on the Risks of Data Siphoning Through Authoritarian Internet Dominance see Lindsay Gorman, "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything" (*Alliance for Securing Democracy*, 27 October 2020) <https://securingdemocracy.gmfus.org/future-internet/> Accessed 25 October 2022.

[431] Xiao Qiang, "Chinese Digital Authoritarianism and Its Global Impact" (2021) 43 Pomeps Studies <https://pomeps.org/wp-content/uploads/2021/08/POMEPS_Studies_43_Draft3-1.pdf#page=36> Accessed 25 October 2022, 39.

[432] Cladiu Codreanu, nº 68, p. 50.

[433] Michael Ceci and Lawrence Rubin, "China's 5G Networks: A Tool for Advancing Digital Authoritarianism Abroad" (2022) 66 Issue 2 270, 276.

[434] Missy Ryan, "Russia spent millions on secret global political campaign, U.S. intelligence finds" *The Washington Post* (Washington D.C, 13 September 2022).

[435] George Parker and Helen Warrell "UK Ministers accused of turning blind eye to any Russian interference" *Financial Times* (London, 21 July 2020).

warfare campaign designed to sow discord in American Politics and Society."[436] These examples clearly show how some authoritarian regimes' impact goes further national borders, which is very concerning to us all.[437] After all, "subsequent elections have been plagued with concerns regarding online disinformation and election-hacking."[438]

Regarding the so-called western democracies, there was a change in paradigm. In fact, as GIOVANNI DE GREGORIO and ROXANA RADU point out "the communication technologies of the 20th century challenged both sovereignty and territoriality, due to their transnational nature and their (almost exclusive) private ownership."[439]

The main companies are American (Meta Group, Microsoft, Amazon, Google) and all of them have in common a desire for "unilateral design of technical and behavioral rules and limited public oversight."[440] ORESTE POLLICINO says that this shows how "powers are relocated among different actors in the information society."[441] The problem is that these private actors have the possibility to block content and websites, remove certain users[442] and disrespect the privacy of citizens.

Therefore, we've come to a moment where it's necessary to balance two different interests: protect fundamental rights and control these platforms' powers,

---

[436] U.S Senate Select Committee on Intelligence "Senate Intel Committee Releases Bipartisan Report on Russia's Use of social media" (8 October 2019).

[437] Having in mind what Patrica Vargas-Leon, "Tracking Internet Shutdown Practices" in Francesa Musiani and others (Ed) *The Turn to Infrastructure in Internet Governance* (Palgrave Macmillan, 2016) 167, 187 says this attempt to control is "an open contradiction with the internet open architecture design, created with the intention of keeping the Internet free of control by one single authority or entity."

[438] Susana Garside, "Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom" (2020) 1/2020 EU Diplomacy Papers <http://aei.pitt.edu/102381/1/edp_1-2020_garside.pdf> accessed 25 October 2022, p. 11.

[439] Giovanni de Gregorio and Roxana Radu, nº 2, p. 75.

[440] *Ibid,* 75.

[441] Oreste Pollicino, "Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and Its possible solution" Early Draft (*European Court of Human Rights,* 2021) < https://echr.coe.int/Documents/Intervention_20210415_Pollicino_Rule_of_Law_ENG.pdf> Accessed 28 October 2022, p. 2.

[442] In 2021, Donald Trump's Twitter account was permanently suspended, after showing support to the people that attacked the capitol. Twitter considered that there was a violation of its terms of conditions. The same also happened with André Ventura. Chega's leader was expelled permanently in 2022, due to the spread of hate. Therefore, the powers that these digital platforms have may have a crucial role in the different systems.

which is leading to a "new wave of (digital) constitutionalism."[443] We cannot forget that these platforms, as private actors, can't be hold accountable in the same way as the States and companies also enjoy the fundamental rights compatible with their nature, such as the right to property recognized by Protocol No.1 of ECHR.[444] As NIVA ELKIN-KOREN and MAAYAN PEREL refer they play a "dual role", because, as commercial players, "compete in data capitalist markets for users[445]" and they also "act as a governor of other people's speech, hence are expected to advance public welfare."[446]

The doctrine identifies two challenges regarding this matter. Firstly, this moderation exercised by platforms circumvents separation of power[447], especially having in mind that this was traditionally the function of public authorities and they act "in the absence of a legal review or judicial order."[448] There is, according to GIOVANNI DE GREGORIO, a "lack of any transparent procedure or redress mechanisms allowing users to appeal against a decision regarding the removal or blocking."[449] Secondly, these decisions are made with different technological measures[450] and we must take into account that there's a risk to make errors. After all, as ORESTE POLLICINO states "algorithms are not necessarily driven by the pursuit of public interests" and may "undermine accountability and the human understanding of the decision-making process."[451]

---

[443] Giovanni de Gregorio, "From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights in the Algorithmic Society" (2019) 11 no 2 European Journal of Legal Studies 65, 68.

[444] It clearly states that "every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law."

[445] Marta Vicente, "XV Encontro de Professores de Direito Público" (9 September 2022) < https://www.youtube.com/watch?v=lUb3nEoF0oc&t=> 42:22-43:, reminds that these platforms rely on publicity and the decisions to remove content have a commercial nature. Therefore, if they decide to remove too much content it'll undermine the interactions between users with the risk of losing them. However, if the platform doesn't remove any content at all, a hostile environment will be created, which may also result in the loss of users.

[446] Niva Elkin-Koren and Maayan Perel, "Guarding the Guardians: Content Moderation by online intermediaries and the rule of law" in Giancarlo Frosio (Ed) *The Oxford Handbook of online intermediary liability* (Oxford University, 2020) 669, p. 671..

[447] *ibid,* 672.

[448] Giovanni de Gregorio, nº 88, p. 82.

[449] *ibid,* 83.

[450] Niva Elkin-Koren and Maayan Perel, nº 92, 672.

[451] Oreste Pollicino, "Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and Its possible solution", p. 6.

Besides these challenges, what intrigues me the most is the duality regarding the accountability of these private actors. If we look into the European example, there's a continuous effort to balance the fundamental rights of citizens and the platform's interests. Recently, Elon Musk bought Twitter and his first tweet stated that "the bird is freed." What's really interesting is Thierry Breton's reaction, European Commissioner, saying that "In Europe, the Bird will fly by our EU rules." This clearly shows the tension when it comes to internet's regulation and the exercise of rights. We've seen before how freedom of expression is perceived in the USA and the contrast that there is when it comes to Europe. I think that GIOVANNI DE GREGORIO and ROXANA RADU have a point when they outline the impact of the constitutional peculiarities when it comes to the internet's regulation. Therefore, in the USA, contrarily to EU, "the US government has opted for consolidating the space for a liberal hub in which American technology giants can thrive on a global scale."[452]

This tension is even more interesting when we analyze these giant tech's reaction. In fact, regarding data protection of users, in February 2022, the Meta Group said it might decide to shut down Facebook and Instagram in Europe, unless a new transatlantic data transfer framework is adopted.[453] As an example, it's important to point out the *Google Spain* Case.[454] Besides the discussion on whether Google was a controller under the Directive 95/46[455], the main topic was to know if Costeja González had the right to have his information regarding his debts to social security deleted. The CJEU held that:

Under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.

There was, for the first time, the recognition of the *right to be forgotten*[456], a clear demonstration of the importance to protect user's rights which, according to GIOVANNI DE GREGORIO, "has unveiled a legal basis for data subjects to enforce

[452] Giovanni de Gregorio and Roxana Radu, nº 2, 83.

[453] Sam Shead, "Meta says it may shut down Facebook and Instagram in Europe over data-sharing dispute" *CNBC* (Englewood, 7 February 2022).

[454] *Google Spain v. Agencia Española de Protección de Dados and Mario Costeja González* (C-131/12) 13 May 2014.

[455] The GRDP was only implemented in 2016.

[456] Regarding the framework of this right, Catarina Botelho, "O Direito ao Esquecimento e o princípio da proporcionalidade no constitutcionalismo global" (2017) V 7 *AB* Instantia 49, 64 considers that the right to be forgotten derives from the right to self-determination, protection to private life, honor, image and name.

their rights against private actors."[457] This was a tremendous step, in order to assure that these powers aren't absolute. Not only the platforms are exercising rights that "normally" would be attributed to the public sphere, but they also have the power to shape our daily life. After all, the terms of conditions are written "in a way to safeguard the commercial interests of platform providers."[458] Consequentially, most times the users, even though they give their consent and accept these terms of conditions, aren't fully aware (because these terms are too ambitious) of how that data will be collected. This is particularly important nowadays, because personal data is "the new oil"[459] and may function as *counter performance*.[460] In the USA, after the Supreme Court's decision to overturn the constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization,* there has been a reasonable concern regarding women's privacy, because from now on there's a risk that their data may be used against them in the states that criminalized abortion.[461]

For these reasons, in order to preserve our democracies, I think it's fundamental that "online intermediaries must be held accountable for content moderation and must comply with the rule of law."[462]

---

[457] Giovanni de Gregorio, nº 88, 83. Indeed this is such an important case law, because it outlines the importance to balance the interests, establishing limits to the "margins of discretion in deciding whether to delist information."

[458] Nicolas Suzor, "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by platforms" (2018) 4(3) *Social Media + Society*< https://journals.sagepub.com/doi/10.1177/2056305118787812> accessed 29 October 2022, p. 3.

[459] Jorge Morais Carvalho, *Direito do Consumo* (Almedina, 7th Edn, 2021) 62.

[460] Regarding this topic, it was adopted the Council Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. Here, it's clearly stated that the "Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trade." (Art. 3º/1). This was another important step to regulate these situations and assure new mechanisms of protection of the users, this time under consumer and data protection law. It's quite interesting because before the adoption of this Directive, the European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on Certain aspects concerning contracts for the supply of digital content* (EDPS, 14 March 2017) considered that the use of the term counter performance wasn't appropriate to address the business models at stake and could appear to oversimplify in one single term a variety of business models and data usages. On the other hand, it stated that this was a misleading concept, because "While the consumer is aware of what he is giving when he pays with money, the same cannot be said about data." *Ibid,* page 9.

[461] Even before the court's decision, women in the USA started to delete their period tracking apps because prosecutors could request the information collected in order to build a case. Flora Garamvolgyi, "Why Women are deleting their period tracking apps" *The Guardian* (London, 28 June 2022).

[462] Niva Elkin-Koren and Maayan Perel, nº 92, p. 674.

5. The role of Digital Constitutionalism

The landscape of constitutionalism has changed. Nowadays, it's impossible to think about fundamental rights without recognizing the importance that the Internet has. When the first written constitutions, during the Liberal movements, were created, we were far from imagining that the way society operates would change significantly. Therefore, constitutionalism itself cannot stay indifferent to those modifications. As EDOARDO CELESTE states, "constitutionalism in undergoing on a mutation on multiple fronts"[463] and this cannot be ignored. GIOVANNI DE GREGORIO identifies three different phases: *1st digital liberalism* (characterized by the establishment of a common market, approximation of policies and regulation of "critical areas for the growth of digital environment)[464], 2nd *judicial activism* (whose existence was due to the emergence of digital environment and new online intermediaries)[465] and 3rd *digital constitutionalism*[466] (a phase characterized by the fact that "public actors are still a primary source of concern but are no longer the only source of interference with individual fundamental rights and freedoms.")[467] This last phase arises from the idea, as we've seen, that private actors play a crucial role in the digital world. The doctrine identifies this as the current main challenge of digital constitutionalism. BRIAN FITZGERALD, even though he was focused on a more private approach, firstly identified that the goal of "informative constitutionalism" would be "an integrative institutional structure that glues together these multi-layered governance or intersecting order-creating mechanisms."[468] NICOLAS SUZOR says that "finding ways to improve the legitimacy of platform governance, through both legal rules and social obligations, is the key challenge and opportunity of digital constitutionalism."[469] I agree with the definition proposed by EDOARDO CELESTE, who considers that "digital

[463] Edoardo Celeste, Digital Constitutionalism: The Role of Internet Bill of Rights (Routledge, 1st Edn, 2022) 81.

[464] Giovanni de Gregorio, Digital Constitutionalism in Europe – Reframing Rights and Powers in the Algorithmic Society (Cambridge University Press, 1st Edn, 2022) 41-52.

[465] ibid, 53-64.

[466] Regarding the concept itself, as Lex G., Dennis Redeker and Urs Gasser, "Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights" (2015) 15 *Berkman Center Research Publication* < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120> Accessed 1 November 2022, state – and, in my point of view, correctly - that there's utility to "framework digital constitutionalism rather than mere digital rights charters."

[467] Giovanni de Gregorio, nº 109, 64

[468] Brian Fitzgerald, "Software as a discourse? A constitutionalism for information society" 24(3) Alternative Law Journal <http://www5.austlii.edu.au/au/journals/AltLawJl/1999/25.html> accessed 2 November 2022.

[469] Nicolas Suzor, nº 103, 9.

constitutionalism is rather the set of values and ideals that permeate, guide and inform this series of instruments."[470]

In 2016, the Human Rights Council adopted Resolution 32/13[471], where it recognized the importance of the "global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms", aiming the states to "bridge the gender digital divide and enhance the use of enabling technology." Would it make sense, nowadays, to create a Global Internet Constitution? Regardless of the answer given, it's unquestionable that "everyone should have the right to exercise their rights according to the standard that new technology and, at the same time, be protected against fundamental rights infringement."[472]

Over the years, some countries have adopted their own version of an Internet Bill of Rights. The First country to adopt a Civil Rights for the Internet was Brazil, in 2014, with Marco Civil[473], a Bill that settled principles, rights and duties for the users, whose creation is considered "an intense manifestation of digital constitutionalism", mainly due to its "formal statute."[474] In 2015, Italy's Parliament proposed a Declaration of Internet Rights, whose document consecrates, the right to *Internet Access, the right to online knowledge and education, protection of personal data, the right to informational self-determination* among others. Another recent example is the Portuguese Charter of Human Rights in the Digital Era[475], whose main goal is to regulate matters related with the digital environment and gives us the ability to consecrate many rights and guarantees, such as the right to internet neutrality, digital class action, the right to privacy or the right to internet's access).[476] In 2021, Sánchez,

---

[470] Edoardo Celleste, "Digital Constitutionalism: a new systematic theorization" (2019) 33(2) International Review of Law Computers & Technology <https://doi.org/10.1080/13600869.2019.1562604> accessed 2 November 2022, 17.

[471] Human Rights Council Resolution Resolution 32/13 "The Promotion, Protection and enjoyment of human rights on the Internet" (18 July 2016) 32th Session Doc Supp number A/HRC/RES/32/13

[472] EDOARDO CELESTE, nº 108., 92.

[473] Marco Civil Law of the Internet in Brazil (23 April 2014) Law number. 12.965

[474] Luiz Moncau and Diego Arguelhes, "The Marco Civil da Internet and Digital Constitutionalism" in Giancarlo Frosio (Ed) *The Oxford HandBook of Online Intermediary Liability* (Oxford University Press 2020) 190, 207. For a better approach regarding the Marco Civil see the article mentioned.

[475] Portuguese Charter of Human Rights in the Digital Era (17 May 2021), Law number 27/2021.

[476] The initial proposal was under fire, because Article 6º foresaw the possibility to create a special structure to verify facts posted on social media. Several political parties raised important questions regarding article 6. Some saw in this article (and, in my opinion, correctly) a way to restraint freedom of expression. In my eyes, facts verification cannot be done at the cost of a fundamental right's limitation. Besides, there would be the risk that this would be used for political or ideological reasons. There are, as it's obvious, less strict ways to achieve the same goal without restraining such freedoms. For example, in Portugal there are several programs

Spain's Prime-Minister, also presented the Digital Rights Charter (*Carta Derechos Digitales*) and it was recognized that this wasn't about creating new fundamental rights, but instead consecrate the most relevant in the digital world. This Charter would function, therefore, as a mere guideline, because it was adopted as a declaration and not as a bill (so it doesn't have binding force).[477]

On the other hand, there are also important initiatives adopted that don't belong to States. One example is *The Charter of Human Rights and Principles for the Internet,* created by the Internet Rights & Principles Dynamic Coalition, an international network of individuals and organizations working to uphold human rights in an online environment.[478]

As EDOARDO CELLESTE states "these documents represent a unique component of the multilevel mosaic of norms that address the constitutional issues of the global society and are currently reacting against the challenges of the digital revolution."[479] In fact, these documents are really impressive, because they abstractly show a will to adapt the exercise of fundamental rights into the digital world (if they'll be effective, that's another story).

Nevertheless, at this moment of transformation, I think it's almost impossible to adopt a universal charter for the internet. There are two problems in this: *(i)* lack of enforcement and *(ii)* difficulty to adopt a consensual document. The adoption of something universal is always hard, but in this case it's even harder (because we're talking about the internet). GIOVANNA DE MINICO[480] raises an important question that is directly related with what I'm discussing. Which authority shall have the legitimacy to write such charter? As the Author argues, the idea of a State must be refused, because "the anti-territorial nature of the internet would be incompatible with an authority entrusted with powers constrained within state boundaries."[481]

On the other hand, if we look at international organizations (UN, for example), it'd be almost impossible to adopt something like this, because, as GIOVANNA DE

---

that verify if a fact is true or false (Polígrafo, Hora da Verdade, Observador's Fact Check). Due to the public debate raised, President Marcelo submitted this to the PCC.

[477] Spain's Government, *Carta Derechos Digitale* (14 July 2021) < https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721Carta_Derechos_Digitales_RedEs.pdf> accessed 2 november 2022.

[478] Internet Rights & Principle Coalition, "The Charter of Human Rights and Principles" (2014) < https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf> accessed 2 November 2022.

[479] EDOARDO CELLESTE, nº 108., 116.

[480] Giovanna de Minico, "Towards na Internet Bill of Rights" (2015) 37(1) *Loyola of Los Angeles International and Comparative Law Review* <https://digitalcommons.lmu.edu/ilr/vol37/iss1/1/> Accessed 1 November 2022, 20.

[481] *ibid,* p. 20.

MINICO states "they fall easily under the influence of strong national states, the interests of which only occasionally coincide with a broader common good."[482] Even if in a perfect world, composed by unicorns and rainbows, the UN was able to create something like that, then it'd be almost impossible to enforce it and the charter would be a dead document (it's almost absurd that countries such as China or Russia, that as we've seen don't respect the most basic fundamental rights, have the veto power within the Security Council).[483]

Regarding this topic, the author proposes a median hypothesis, stating that the legislative power should be "vested in a public supranational authoritative body, based on legal and binding provisions; which also defines the nature and scope of its powers"[484] and that decision-making process should include the representation of private interests. Well, I still find it difficult to foresee something like this. In fact, the author's proposal has its merits, but even if it was possible to come to this point, there would be no guarantees regarding the enforcement of this charter and I still don't quite understand how the states will recognize legitimacy for its draft. On the other hand, even if we're able to recognize some of the fundamental rights inherent to the internet's use (some of the charter mentioned above consecrate identical rights such as the right to internet's access, right to be forgotten in some, the right not to be discriminated, among others), it'll be missing something important: how that should be engaged with private actors, particularly having in mind that they play an important role nowadays.

For this reason, GIOVANNI DE MINICO proposes that they should be part of this making process, which isn't enough, in my opinion, because, as private companies, they'll always try to follow their interests (which is legitimate, because they aim for the profit). Nevertheless, we mustn't forget that "the process of constitutionalisation does not adopt a single modality, but it is translated into different normative answers"[485]

As EDOARDO CELESTE states, these different interventions at a national, regional and even with non-state dimension, demonstrate an ongoing process, which doesn't exclusively "involve a formal institutionalization or codification of norms in binding legal texts", rather, it's a broader process, which starts "from the phase of discussion and elaboration of new constitutional principles at societal level."[486] We're far away from adopting an Universal Charter for the Internet (with binding effects), but this continuous effort made by states, non-governmental institutes show us that digital

[482] *ibid,* p. 20.

[483] This doesn't mean, however, that the USA don't follow their own interests. Many decisions are made taking into account not the interest of the organization as a whole, but having in mind the interests of some countries. After all, it's politics and we cannot change that.

[484] Giovanna de Minico, nº 125, 22.

[485] EDOARDO CELESTE, nº115, 14

[486] *ibid.,* 17.

constitutionalism is the key to inspire an effective change. Therefore, as GIOVANNI DE GREGORIO and ROXANA RADU point out, from now on, the "primary challenge for digital constitutionalism is to ensure not only that public interferences online are minimized, but also that the public-private cooperation is brought in line with the constitutional values underpinning fundamental rights and democracy."[487]

6. Conclusion

The internet plays a crucial role in our society. Considered by many the new "public forum", it raises important questions regarding the protection of fundamental rights in the digital world. Due to its importance, many countries around the world have tried to shape and control the internet, mainly with the intention to increase censorship and limit fundamental freedoms. This isn't ideal and may be dangerous to western countries. However, it'd be utopic to consider that these democracies don't face different challenges, namely the cooperation between public and private authorities when it comes to the digital world. In many cases, these private actors exercise powers that may lead to real restrictions of fundamental rights. Therefore, the challenge in these countries is to find a solution that allows the articulation of the main interests at hand: the rights of citizens and the rights that these companies have. Furthermore, digital constitutionalism is a reality and it'll continue to play an important role in the future.

Reference List

ASENSIO, Pedro - Conflict *of Laws and The Internet* (Edwards Elgar Publishing, 2020).

AZELMAT, Marwa - Marwa Azelmat, "The rise of digital authoritarianism: is the internet to be Blamed" (European Master's Degree in Human Rights and Democratization, Queen's University of Belfast, 2019).

BOTELHO, Catarina Santos

"Transnational Constitutional Law" in Grote, R., Lachenmann,F, and Wolfrum, R, (eds) Max Planck Encyclopedia of Comparative Constitutional Law (Oxford University Press, 2020), forthcoming at https://oxcon.ouplaw.com/

"Comparative Constitutional Studies 2.0 – Lost in Translations Revisited" in Rita Lobo Xavier et al (Ed) *Constitucionalismos e (con)temporaneidade Estudos em Homenagem ao Prof. Doutor Manuel Afonso Vaz* (Universidade Católica Editora, 2020, Porto)

"Is There a Middle Ground Between Constitutional Patriotism and Constitutional Cosmopolitanism? The Portuguese Constitutional Court and the Use of Foreign (Case)

[487] GIOVANNI DE GREGORIO and ROXANA RADU, nº 2, 86.

Law" in Giuseppe Franco Ferrari (Ed.), *Judicial Cosmopolitanism - The Use of Foreign Law in Contemporary Constitutional Systems* (Brill Nijhoff, 2019)

"O Direito ao Esquecimento e o princípio da proporcionalidade no constitutcionalismo global" (2017) V 7 *AB* Instantia

CARVALHO, Jorge Morais - *Direito do Consumo* (Almedina, 7th Edn, 2021)

CECI, Michael and Lawrence Rubin, "China's 5G Networks: A Tool for Advancing Digital Authoritarianism Abroad" (2022) 66 Issue 2

CELESTE, Edoardo

Digital Constitutionalism: The Role of Internet Bill of Rights (Routledge, 1st Edn, 2022)

"Digital Constitutionalism: a new systematic theorization" (2019) 33(2) *International Review of Law Computers & Technology* <https://doi.org/10.1080/13600869.2019.1562604> accessed 2 November 2022

CODREANU, Claudiu - "Using and Exporting Digital Authoritarianism: Challenging both cyberspace and democracies" (2022) 16 1 *Europolity* 39

FASSBENDER, Bardo - "The United Nations Charter as the Constitution of the International Community" (1998) 36 No. 3 Columbia Journal of International Law

FITZGERALD, Brian - "Software as a discourse? A constitutionalism for information society" 24(3) *Alternative Law Journal* <http://www5.austlii.edu.au/au/journals/AltLawJl/1999/25.html> accessed 2 November 2022.

FLORIDI, Luciano - "The Fight for Digital Sovereignty: What it is, and why it matters, especially for the EU" (2020) 33 Philosophy & Technology, 369, < https://link.springer.com/article/10.1007/s13347-020-00423-6 > Accessed 2 November 2019

FREDERICK, Erixon and and Hosuk Lee-Makiyama, "Digital Authoritarianism: Human Rights, Geopolitics and commerce" (2011) 5/2011 EUROPEAN Center for International Political Economy <https://www.econstor.eu/bitstream/10419/174715/1/ecipe-op-2011-5.pdf> accessed 25 October 2022

GORMAN, Lindsay - , "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything" (*Alliance for Securing Democracy*, 27 October 2020) <https://securingdemocracy.gmfus.org/future-internet/> Accessed 25 October 2022.

GREENBER, Marc - "A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market" (2003) 18 Berkeley Technology Law Journal (Berkeley Tech.L.J.)

GUADAMUZ, Andrés - "Internet Regulation" in Lilian Edwards (ed), *Policy and The Internet Law* (Hart Publishing, 2018)

GREGORIO, Giovanni de

"From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights in the Algorithmic Society" (2019) 11 no 2 European Journal of Legal Studies.

Digital Constitutionalism in Europe – Reframing Rights and Powers in the Algorithmic Society (Cambridge University Press, 1st Edn, 2022)

GREGORIO, Giovanni de and Roxana Radu - Digital Constitutionalism in the new era of internet governance" (2022) 30 Issue 1 International Journal of Law and Information Technology, 68

HAUPT, Claudia - Regulating Speech Online: Free Speech Values in Constitutional Frames" (2021) 99 Nbr 2 Wash. U. L. Rev. 751.

ISFAHANI, Sayeh -"The Internet Protection Bill will hurt all Iranians, but the queer community will have the most to lose" (*Atlantic Council* 12 April 2022) <https://www.atlanticcouncil.org/blogs/iransource/the-internet-protection-bill-will-hurt-all-iranians-but-the-queer-community-will-have-the-most-to-lose/> accessed 15 October 2022

KHALIL, Lydia - "Digital Authoritarianism, China and COVID" (*Institute for International Policy,* 2020) <https://www.lowyinstitute.org/sites/default/files/Khalil%2C%20Digital%20Authoritarianism%2C%20China%20and%20Covid_web_print_021120.pdf> accessed 24 October 2022

KOREN, Niva Elkin and Maayan Perel, "Guarding the Guardians: Content Moderation by online intermediaries and the rule of law" in Giancarlo Frosio (Ed) *The Oxford Handbook of online intermediary liability* (Oxford University, 2020) 669.

LEON, Patrica Vargas- "Tracking Internet Shutdown Practices" in Francesa Musiani and others (Ed) *The Turn to Infrastructure in Internet Governance* (Palgrave Macmillan, 2016) 167.

LIN, Elbert "Prioritizing Privacy: A Constitutional Response to the Internet" (2002) 17 Number 3 Berkeley Tech.L.J 1085.

LODDER, Arno R. -"Internet Law: A Brief Introduction" in Barney-Warf (ed) *SAGE Encyclopedia of the Internet* (2018) <https://ssrn.com/abstract=3191751> accessed 25 October 2022.

MINICO, Giovanna - "Towards na Internet Bill of Rights" (2015) 37(1) *Loyola of Los Angeles International and Comparative Law Review* <https://digitalcommons.lmu.edu/ilr/vol37/iss1/1/> Accessed 1 November 2022, 20.

MIR, Joan and Marco Bassini, "Freedom of Expression in the Internet" in Oreste Pollicino and Graziella Romeo (eds) *The Internet and Constitutional Law – The Protection of Fundamental Rights and Constitutional Adjudication in Europe (*Routledge, 2016).

MONCAU, Luiz and Diego Arguelhes, "The Marco Civil da Internet and Digital Constitutionalism" in Giancarlo Frosio (Ed) *The Oxford HandBook of Online Intermediary Liability* (Oxford University Press 2020).

QIANG, Xiao "Chinese Digital Authoritarianism and Its Global Impact" (2021) 43 Pomeps Studies <https://pomeps.org/wp-content/uploads/2021/08/POMEPS_Studies_43_Draft3-1.pdf#page=36> Accessed 25 October 2022.

SCHAUER, Frederick -"Freedom of Expression Adjudication" in George Nolte (Ed.) *European and US Constitutionalism* (Cambridge University Press, 2005).

PETTERS, Anne - Transnational Law comprises Constitutional, Criminal and Quasi-Private Law in Pieter Bekker *et al Making Transnational Law work in the global economy* (Cambridge University, 2010), 154.

PEREIRA, Alexandre - "Direito ao respeito pela vida privada digital" in Paulo Pinto de Albuquerque (Ed) *Comentário da Convenção Europeia dos Direito Humanos e dos Protocolos Adicionais – Volume II* (Universidade Católica Editora, 2019), 1451.

POLLICINO, Oreste

- *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart Publishing 2021)

- "Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and Its possible solution" Early Draft (European Court of Human Rights, 2021) < https://echr.coe.int/Documents/Intervention_20210415_Pollicino_Rule_of_Law_ENG.pdf> Accessed 28 October 2022.

POLLICINO, Oreste and Gaziella Romeo - , "Internet Law, Protection of Fundamental Rights and the role of Constitutional Adjudication" in Oreste Pollicino and Graziella Romeo (eds) *The Internet and Constitutional Law – The Protection Fundamental Rights and Constitutional Adjudication in Europe* (Routledge, 2016).

POLLICINO, Oreste and Marco Bassini - The Law of The Internet: Between Globalization and Localization" in Miguel Poiares Maduro *et al* (Ed) *Transnational Law – Rethinking European Law and Legal Thinking* (Cambridge University Press, 2014).

PORTARU, Adina - Freedom of Expression Online – The Code of Conduct on Countering Illegal Hate Speech Online" (2017) 4 Romanian Review of European Law, 77.

RAMCHARAN, B. - *The Concept and Present Status of the International Protection of Human Rights – Forty years after the Universal Declaration* (Nijhoff Publishers, 1989).

REDEKER, Dennis, Lex G., and Urs Gasser, "Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights" (2015) 15 *Berkman Center Research Publication* < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120> Accessed 1 November 2022

ROWBOTOOM, Jacob - "The Protection of Expression in the UK" in Oreste Pollicino and Graziella Romeo (Eds) *The Internet and Constitutional Law – The Protection of Fundamental Rights and Constitutional Adjudication in* Europe (Routledge, 2016) 192.

RUSTAD, Michael J. - *Global Internet Law* (Third Edn, West Academic Publishing, 2020).

SHERMAN, Justin - "Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior" (*The Atlantic Council,* 12 July 2021) < https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/> accessed 14 October 2022.

SUZOR, Nicolas - "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by platforms" (2018) 4(3) *Social Media + Society*< https://journals.sagepub.com/doi/10.1177/2056305118787812> accessed 29 October 2022.

VICENTE, Marta - "XV Encontro de Professores de Direito Público" (9 September 2022) < https://www.youtube.com/watch?v=lUb3nEoF0oc&t=> Accessed 30 October 2022

VOLOKH, Eugene - First Amendment Protection for Search Engine Search Results" (2012) 12(22) *UCLA School of Law Research Paper.*

WALKER, Neil - "Constitutionalism and Pluralism in Global Context" in *Constitutional Pluralism in the European Union and Beyond* (Hart Publishing, 2012).

YABOKE, Erol - "Promote and Build a Strategic Approach to Digital Authoritarianism" (*Center for Strategic International Studies,* October 2020) <https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism > Accessed 24 October 2022.

YEH, Jiunn-Rong and Wen-Chen Chang - "The Emergence of Transnational Constitutionalism: Its features, Challenges and Solutions" (2008) 27 No 1 Penn State Law Review, 89.

Case Law

Ahmet Yildirim v Turkey Application number 3111/10 (ECtHR, 18 December 2012).

Cengiz and Others v. Turkey, Application 48226/10 and 14027/11 (ECtHR, 1 December 2015).

Vladimir Kharitonov v. Russia Application 10795/14 (ECtHR, 23 June 2020).

Delfi AS v. Estonia Application number 64569/09 (ECtHR, 10 October 2013)

Big Brother Watch and Others v. United Kingdom, Application number 58170/13, 62322/14 and 24960/15, (ECtHR 25 may 2011).

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application number. 62540/00 (ECtHR 28 June 2007).

Digital Rights Ireland Ltd (C-293/12) 8 April 2014.

Delfi AS v. Estonia Application number 64569/09 (ECtHR, 10 October 2013).

West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624 (1943).

Cohen v. California, 403 U.S. 15 (1971).

Buckley v. Valeo, 424 U.S. 1 (1976).

Virginia v. Black, 538 U.S. 343 (2003).

United States v. Williams, 553 U.S. 285 (2008).

Morse v. Frederick, 551 U.S. 393 (2007).

Packingham v. North Carolina, 582 US, (2017).

II
Outros Estudos

Releitura da Função Judicial no Neoconstitucionalismo – uma análise da atuação do Supremo Tribunal Federal Brasileiro

Renata Guilardi de Oliveira Castro[488]

Resumo
A ideia da separação dos poderes não tinha como objetivo atribuir ao Poder Judicial visibilidade, mas ao exercer o controlo da constitucionalidade das leis, esse Poder foi assumindo cada vez mais importância política, dando ensejo ao chamado neoconstitucionalismo, adotado pelo Poder Judicial brasileiro, que age como legislador negativo e positivo ao utilizar, tanto no controlo concreto quanto no controlo abstrato das leis, a metodologia da aplicação direta dos princípios para determinar a validade e a interpretação das leis. Se teoricamente há fundamento para essa atuação do Poder Judicial, mais especificamente do Supremo Tribunal

[488] Mestranda em Direito Judiciário na Universidade Européia, é advogada (no Brasil e em Portugal); cursou Direito na Pontifícia Universidade Católica de Goiás e Pós Graduação em Direito Administrativo Contemporâneo no Instituto de Direito Administrativo de Goiás; no Brasil exerceu o cargo de assessora jurídica: no Ministério Público do Estado de Goiás entre 1999 e 2006, e no Tribunal de Justiça do Estado de Goiás entre 2006 e 2014. Carreira de docência universitária no curso de Direito entre 2004 e 2022 na Pontifícia Universidade Católica de Goiás; na Associação Objetiva de Ensino Superior e na Associação Goiana de Ensino – Uni-Goiás.

Federal, sem ocorrer ofensa ao princípio da separação dos poderes, algumas decisões desse órgão, pela repercussão política, vêm ensejando questionamentos acerca da legitimidade e a adjetivação de ativismo judicial. Mas será que esse órgão realmente está extrapolando sua função precípua?

Palavras chaves: Separação de Poderes. Ativismo Judicial. Judicialização da Política.

Releitura da Função Judicial no Neoconstitucionalismo – uma análise da atuação do Supremo Tribunal Federal Brasileiro

Renata Guilardi de Oliveira Castro

Abstract
The idea of separation of powers was not intended to give visibility to the Judiciary, but by exercising control over the constitutionality of laws, this Power took on increasingly more political importance, giving rise to the so-called neoconstitutionalism, adopted by the Brazilian Judiciary, which acts as a negative and positive legislator when using, both in concrete and abstract control of laws, the methodology of direct application of principles to determine the validity and interpretation of laws. If theoretically there is a basis for this action by the Judiciary, more specifically the Federal Supreme Court, without causing an offense to the principle of separation of powers, some decisions of this body, due to political repercussion, have given rise to questions about the legitimacy and the adjective of judicial activism. But is this organ really going beyond its primary function?

Keywords: Separation of Powers. Judicial activism. Judicialization of Politics.

Introdução

É consequência de um país considerado continental, como o Brasil, em razão de sua extensão territorial (área de 8.514.876 km² conforme o *site* ibge.gov.br), e que contém regiões tão diferentes, tanto sob o aspecto cultural quanto social e econômico, que ocorram conflitos de natureza bem diversificada, e a judicialização desses conflitos traz visibilidade ao Poder Judicial, pois é cláusula pétrea na CRFB/88, que "*a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;*" (artigo 5º, XXXV).

Todavia, no Brasil a legitimidade do Supremo Tribunal Federal vem sendo questionada porque a ideia da separação dos poderes concebida a partir de um Poder Judicial nulo e invisível não converge com a atual posição desse órgão, que gradativamente vem alcançando um patamar de relevância e autoridade político-normativa, se tornando um participante ativo na formação de políticas públicas e na condução do processo democrático brasileiro através, principalmente, do controlo abstrato das normas.

Sobre esse tipo de controlo, a competência do Supremo Tribunal Federal pode ser exercida através de vários mecanismos como: a Ação Direta de Inconstitucionalidade – ADI, a Ação Declaratória de Constitucionalidade – ADC; Arguição de Descumprimento de Preceito Fundamental – ADPF e Ação Declaratória de Inconstitucionalidade por Omissão.

Como a legitimidade ativa para propor essas ações constitucionais de controlo abstrato são de órgãos dos poderes Executivo e Legislativo, além do Ministério Público, Ordem dos Advogados e partidos políticos[489], o Supremo Tribunal

[489] Art. 103. Podem propor a ação direta de inconstitucionalidade e a ação declaratória de constitucionalidade:

I - o Presidente da República;

Federal vem sendo chamado a tratar de temas polêmicos, sendo usado, inclusivamente, para dirimir conflitos existentes entre os Poderes Legislativo e Executivo, razão pela qual vem sendo "acusado" de ativismo judicial.

A título de exemplo, em 2018 o Supremo Tribunal Federal foi censurado pelo Comitê de Direitos Humanos da Organização das Nações Unidas, em razão de uma decisão que refletiu nas eleições presidenciais daquele ano.

Estava em curso a "Operação Lava Jato", que envolvia políticos e empresários em esquemas de corrupção. O então ex-Presidente da República, Luiz Inácio Lula da Silva, foi processado e condenado pela Justiça Federal de Curitiba em 12/07/2017 e a condenação foi confirmada em segunda instância pelo Tribunal Regional Federal em abril de 2018, mas sem trânsito em julgado porque ainda foram interpostos dois recursos, um perante o Superior Tribunal de Justiça e outro perante o Supremo Tribunal Federal.

O que parece estranho é que, de 2009 a 2016, o entendimento do Supremo Tribunal Federal era no sentido de proibir o início da execução da pena antes do seu trânsito em julgado, sob o argumento de que lesava o princípio constitucional da presunção de inocência, mas durante a "Operação Lava Jato", esse órgão mudou o entendimento, passando a admitir a execução da pena não transitada em julgado, desde que ratificada em segunda instância. Por isso, quando a condenação do ex- Presidente Lula foi confirmada em segunda instância, em 07 de abril de 2018, ele foi preso e teve seus direitos políticos suspensos, não podendo concorrer às eleições presidenciais de 2018.

II - a Mesa do Senado Federal;

III - a Mesa da Câmara dos Deputados;

IV a Mesa de Assembléia Legislativa ou da Câmara Legislativa do Distrito Federal;

V o Governador de Estado ou do Distrito Federal;

VI - o Procurador-Geral da República;

VII - o Conselho Federal da Ordem dos Advogados do Brasil;

VIII - partido político com representação no Congresso Nacional;

IX - confederação sindical ou entidade de classe de âmbito nacional.

§ 2º Declarada a inconstitucionalidade por omissão de medida para tornar efetiva norma constitucional, será dada ciência ao Poder competente para a adoção das providências necessárias e, em se tratando de órgão administrativo, para fazê-lo em trinta dias.

Pelo fato do Supremo Tribunal Federal ter "mudado de ideia" o Partido Patriota e o Conselho Federal da Ordem dos Advogados do Brasil ajuizaram as Ações Declaratórias de Constitucionalidade nº. 43 e nº. 44, almejando a declaração de que o artigo nº. 283 do Código de Processo Penal Brasileiro era constitucional ao exigir o trânsito em julgado da sentença penal como marco inicial para a execução penal. Em abril de 2018, o Partido Comunista do Brasil ajuizou a ADC nº. 54, com o mesmo pedido das ADC nº. 43 e nº. 44, incluindo o pedido de efeito vinculante, ou seja, a ser observado obrigatoriamente por todos os Tribunais.

Diante da semelhança das ações, o julgamento das Ações Declaratórias de Constitucionalidade nº. 43, nº. 44 e nº. 54 se deu conjuntamente em Plenário, com início no mês de outubro e término no mês de novembro do ano de 2019. O acórdão do Supremo Tribunal Federal, por 06 votos a 05, declarou a constitucionalidade do artigo 283, do Código de Processo Penal Brasileiro, ou seja, alterou novamente o seu entendimento, deixando de permitir a execução provisória da pena.[490] Em razão desse julgamento, o ex-Presidente Lula foi solto e teve seus direitos políticos restabelecidos em novembro de 2019, mas as eleições presidenciais já haviam passado.

Nesse ínterim, em agosto de 2018, o Comitê de Direitos Humanos da Organização das Nações Unidas (ONU) solicitou ao Brasil que fosse garantido ao Senhor Lula o direito de exercer seus direitos políticos enquanto estivesse preso provisoriamente, "pedido" que não foi atendido pelo Supremo Tribunal Federal. Em 28 de abril de 2022, o Comitê de Direitos Humanos da ONU concluiu que o Senhor Lula teve seus direitos políticos violados em 2018, após ter sido impedido de participar das eleições presidenciáveis daquele ano.

Outro julgado emblemático do Supremo Tribunal Federal é o da ADPF 45/2004, cuja ementa é a seguinte:

> *EMENTA: ARGÜIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL.* ***A QUESTÃO DA LEGITIMIDADE CONSTITUCIONAL DO CONTROLE E DA INTERVENÇÃO DO PODER JUDICIÁRIO EM TEMA DE IMPLEMENTAÇÃO DE POLÍTICAS PÚBLICAS, QUANDO CONFIGURADA HIPÓTESE DE ABUSIVIDADE GOVERNAMENTAL. DIMENSÃO POLÍTICA DA JURISDIÇÃO CONSTITUCIONAL ATRIBUÍDA AO SUPREMO TRIBUNAL FEDERAL.*** *INOPONIBILIDADE DO ARBÍTRIO ESTATAL À EFETIVAÇÃO DOS DIREITOS SOCIAIS, ECONÔMICOS E CULTURAIS. CARÁTER RELATIVO DA LIBERDADE DE CONFORMAÇÃO DO LEGISLADOR. CONSIDERAÇÕES EM*

[490] Voto nas ADCs 43, 44 e 54[1] (poder360.com.br)

TORNO DA CLÁUSULA DA "RESERVA DO POSSÍVEL". NECESSIDADE DE PRESERVAÇÃO, EM FAVOR DOS INDIVÍDUOS, DA INTEGRIDADE E DA INTANGIBILIDADE DO NÚCLEO CONSUBSTANCIADOR DO "MÍNIMO EXISTENCIAL". VIABILIDADE INSTRUMENTAL DA ARGÜIÇÃO DE DESCUMPRIMENTO NO PROCESSO DE CONCRETIZAÇÃO DAS LIBERDADES POSITIVAS (DIREITOS CONSTITUCIONAIS DE SEGUNDA GERAÇÃO).

Por fim, o Supremo Tribunal Federal, nos julgamentos das Ações Declaratórias de Inconstitucionalidade por Omissão, quando procedentes, além de dar ciência ao Poder omisso, em vários casos também determina como o preceito constitucional será aplicado até a omissão legislativa ser sanada.

Ressalta-se que o artigo 103, §2º, da CRFB/88, assim preconiza: *Declarada a inconstitucionalidade por omissão de medida para tornar efetiva norma constitucional,* ***será dada ciência ao Poder competente para a adoção das providências necessárias*** *e, em se tratando de órgão administrativo, para fazê-lo em trinta dias.*

Exemplo dessa conduta é o julgamento da Ação Direta de Inconstitucionalidade por Omissão – ADO 26/DF, datado de 13/06/2019, no qual o Supremo Tribunal Federal a julgou procedente, com eficácia geral e efeito vinculante e, para além de declarar a omissão normativa do Poder Legislativo, cientificando o Congresso Nacional para a adoção das providências necessárias, determinou que, enquanto a omissão não fosse sanada, a homofobia e a transfobia seriam consideradas crimes de racismo, nos termos da Lei nº 7.716/89.[491]

A presente reflexão visa analisar se as críticas à atuação do Supremo Tribunal Federal têm pertinência, ou seja, se está havendo desrespeito ao princípio da separação e interdependeência de poderes e tal análise será feito pela metodologia de pesquisa bibliográfica em bases de dados de publicações científicas, normas, jurisprudências e doutrinas.

1. Breves considerações sobre a separação dos poderes

A questão do controlo do poder político não é uma novidade. Aristóteles já se preocupava com a concentração de poderes em uma só pessoa. Para ele, o poder

[491] https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754019240

deveria ser dividido de forma equilibrada e as instituições políticas não deveriam ficar dependentes das virtudes de seus ocupantes.

Esse filósofo grego tentou sistematizar de forma didática as formas de governo (monarquia, aristocracia e democracia), sem apontar um modelo ideal, imputando aos detentores do poder a responsabilidade de agir de acordo com o bem comum, sob pena do governo em questão se transformar em tirania, oligarquia ou demagogia, respetivamente. Para evitar isso, ressaltou a importância da divisão de funções.

Segundo ele, para um bom governo deveria haver o bom funcionamento de três funções distintas: a que deliberava acerca dos negócios públicos; a que exercia a magistratura (uma espécie de função executiva) e a que administrava a justiça. Aristóteles não chegou a formular uma teoria da separação dos poderes do Estado, mas fez um esboço. Seu contributo foi demonstrar a existência de funções distintas no governo, além de enfatizar o perigo de se atribuir a um só Ente o exercício do poder.

John Locke (1632-1704), partindo da conceção de Aristóteles de que o homem é por natureza um animal político, concebeu a origem da sociedade política, ressaltando a necessidade de divisão equilibrada de poderes para o bom governo. A instabilidade política na segunda metade do século XVII na Inglaterra, especialmente com a sucessão do rei Carlos II, foram os eventos que marcaram a escrita de Dois tratados sobre o governo civil.

O objetivo de Locke, em Dois Tratados sobre o Governo, foi defender a Revolução Gloriosa, decorrente da pretensão absolutista da dinastia Stuart que visava acabar com o governo misto (monarquia e parlamento). Essa Revolução restabeleceu o governo misto, tendo, o parlamento, independência orgânico-funcional em relação ao monarca. Locke fundamentou a Revolução Gloriosa no direito de resistência, pelo qual seu titular, o povo, poderia dissolver a sociedade política e instituir um novo poder político, quando o governante se desviasse do bem comum.

O ponto de partida e o fator último do pensamento de Locke é a natureza do homem, que, segundo ele, nascia livre e com direitos iguais (não na concepção atual). Para ele, no estado de natureza há igualdade e liberdade, mas, justamente para assegurar a vida, a liberdade e a propriedade existentes no estado de natureza era preciso constituir a sociedade civil, mediante um contrato social que só seria

legítimo se sua constituição fosse baseada no livre consentimento dos indivíduos para estabelecer um poder político. Assim, o poder civil seria a derivação do poder natural dos homens e não um poder originário e, de posse desse poder, o Estado criaria leis com o objetivo de preservar os direitos naturais do homem. Esse poder político só poderia ser exercido com o consentimento dos governados e, para assegurar a liberdade e a propriedade, deveria ter uma lei estabelecida pelo consentimento da maioria; ter um juiz conhecido e imparcial com autoridade para solucionar as controvérsias; e ter um poder para apoiar e sustentar e dar à sentença a devida execução.

Para Locke, a divisão do poder político era uma garantia contra a tirania, por isso o dividiu em Legislativo, Executivo e Federativo. Não há menção ao Poder Judicial como poder autônomo, mas, ao fazer menção à importância de um juiz previamente designado e imparcial para assegurar a liberdade e a propriedade do homem, deixou seu contributo para o tema em estudo. O pensamento empírico de Locke influenciou as bases das democracias liberais a ponto de, no século XVIII, os iluministas franceses terem se inspirado nele.

Foi a Inglaterra da pós-Revolução Gloriosa que inspirou Montesquieu, na primeira metade do século XVIII, a conceber a teoria da "separação de poderes", tendo como objetivo criticar o absolutismo francês em prol de uma monarquia moderada, exercida com o auxílio e participação da aristocracia no Parlamento, de acordo com regras preestabelecidas.

Montesquieu, percebendo o Estado como uno, mas composto por diversidades, não visava a separação dos poderes, mas a separação das funções do Estado para evitar confusão entre os poderes legislativo e executivo. Quanto ao poder judicial, considerava que não era um poder político, como os outros, o que lhe conferia independência ao julgar conforme a lei, que, para ele, não era apenas a lei formal, de conotação política, mas incluía a lei natural, da natureza das coisas.[492]

Para ele é histórico que o homem que possui poder é levado a abusar dele e esse abuso coloca em risco a liberdade política, por isso, o poder deve limitar o poder, sendo temerário que o mesmo "homem" acumule o poder de fazer as leis, o

[492] Torres, Miguel Ayuso. El desgobieno de los jueces. Revista de Derecho Público 81, Universidad de Chile, 2014.

poder de executar as resoluções públicas e o poder de julgar. O poder, apesar de uno, não pode estar concentrado em apenas uma pessoa, daí a importância da "separação" dos poderes.

No seu livro O Espírito das Leis, concebeu a tríade adotada pela ciência política moderna: poderes Executivo, Legislativo e Judicial. O Poder Legislativo bicameral (com uma câmara reservada à nobreza e outra aos representantes eleitos por cada comunidade), com a função de estabelecer as normas gerais disciplinadoras da liberdade dos indivíduos. O Executivo, que deveria estar concentrado em uma única pessoa com a função de administrar a coisa pública e o Poder Judicial, que não seria composto de juízes profissionalizados e permanentes, mas sim por jurados escolhidos no povo.

Dessa forma idealizou-se um Poder Judicial invisível e nulo, ou negativo, dentro da perspectiva da política, restando, como Poderes de fato (positivos/políticos), o Legislativo e Executivo.

No final do século XVIII, os revolucionários franceses invocaram a teoria de Montesquieu, mas deram-lhe a interpretação de que o Poder Judicial nulo e invisível se limitava a aplicar as leis nos casos concretos, sem qualquer tipo de interpretação (juiz como a boca da lei em sentido estrito).

Vale ressaltar que a teoria da separação de poderes foi consolidada pelo artigo 16 da Declaração Francesa dos Direitos do Homem e do Cidadão (1789).

Com influência de Locke ao prever o consentimento dos governados para a constituição do governo e o direito do povo de resistir contra os governos desvirtuados do interesse público, a Constituição Norte-Americana de 1787 adotou a República como forma de governo sendo o Poder Executivo ocupado pelo Presidente da República eleito, através de uma democracia representativa, para um mandato de tempo certo e com responsabilidade política.

A teoria da divisão dos poderes foi adotada na Constituição Norte-Americana, com divisão orgânica-funcional entre os três poderes para que uma mesma pessoa ficasse impedida de exercer concomitantemente cargos em Poderes diversos, adotando o sistema de pesos e contrapesos. No Federalista n. 51 de 06 de fevereiro de 1788, Madison (1788) justificou esse sistema, que permite uma certa

interferência de um poder no outro, dentro de limites estabelecidos, para manter o equilíbrio entre eles:[493]

> *To the People of the State of New-York.*
>
> *TO what expedient then shall we finally resort for maintaining in practice the necessary partition of power among the several departments, as laid down in the constitution? The only answer that can be given is, that as all these exterior provisions are found to be inadequate, the defect must be supplied, by so contriving the interior structure of the government, as that its several constituent parts may, by their mutual relations, be the means of keeping each other in their proper places.*

Com inspiração na Constituição Norte-Americana de 1787 foi elaborada a primeira Constituição Republicana dos "Estados Unidos do Brasil", em 1891 (República Federativa), que adotou a divisão de poderes pelo sistema de freios e contrapesos do modelo norte-americano.

Conforme dispõe a atual Constituição da República Federativa do Brasil de 1988 (CRFB/88), o Brasil é uma República Federativa organizada sob o princípio da **separação e interdependência dos poderes**, que é a base de sua constituição como um Estado Democrático de Direito, como se observa da leitura do seu artigo 2º: "*São Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário*".

Ressalta-se que o princípio da separação e interdependência dos poderes está intimamente ligado com governo representativo, onde há a separação entre o exercício do poder pelo povo através das eleições e o exercício do poder pelos governantes; sendo do parlamento, de composição pluralista e representativa do povo, a competência legislativa; onde há independência dos tribunais; enfim, há uma pluralidade de órgãos de função política, com suas respetivas competências definidas pelas normas, a fim de haver um controlo e limitação de poder, com as particularidades decorrentes da evolução dos tempos a partir do século XIX.[494]

---

[493] https://founders.archives.gov/documents/Hamilton/01-04-02-0199

[494] https://www.mprj.mp.br/documents/20184/1250715/Jorge_Miranda.pdf

2. Da Supremacia da Constituição

Conforme preconiza Jorge Miranda, no livro Teoria da Constituição, esta, atualmente, mais do que a institucionalização do ordenamento estatal, é também a racionalização das relações políticas, ou seja, é a fundação e a fundamentação do poder público e de toda a ordem jurídica.

Essa ideia de supremacia vem desde as revoluções americana e francesa, apesar dos respetivos contextos históricos e motivações serem diferentes: nos Estados Unidos foi o ato constitutivo da União e norma fundamentadora do sistema jurídico, e na Europa, o caminho foi mais longo porque havia a preocupação de reestruturar o poder político decorrente do absolutismo monárquico e mitigar a força da lei ordinária, que era tida como a expressão da vontade geral, talvez por isso a fiscalização jurisdicional da constitucionalidade surgiu apenas no século XX.

Nesse sentido, esse autor transcreve as palavras de Hamilton, extraídas da tradução portuguesa de 1984 do *The Federalist Papers (1787)* e de Sieyés, extraída da edição de 1970 de Roberto Zapperi, respectivamente:

> *"Nenhum ato legislativo contrário à Constituição pode ser válido. Negar isto seria como que sustentar que o procurador é maior que o mandante, que os representantes do povo são superiores a esse mesmo povo, que aqueles que agem em virtude de poderes concedidos podem fazer não só o que eles autorizam mas também aquilo que proíbem. O corpo legislativo não é o juiz constitucional das suas atribuições.* ***Torna-se mais razoável admitir os tribunais como elementos colocados entre o povo e o corpo legislativo, a fim de manterem este dentro dos limites do seu poder.*** *Portanto, a verificar-se uma inconciliável divergência entre a Constituição e uma lei deliberada pelo órgão legislativo, entre uma lei superior e uma lei inferior, tem de prevalecer a Constituição"*[495]
> *"A Constituição não é obra do poder constituído, mas sim do poder constituinte. Nenhum poder delegado pode alterar as condições da sua delegação"*

A teoria da estrutura escalonada da ordem jurídica de Hans Kelsen coloca no topo a norma fundamental e, de acordo com ela, se produz a Constituição, que, por sua vez, valida a produção de normas de escalão inferior, geralmente gerais e que também validam a produção de normas hierarquicamente inferiores, que geralmente são individuais. A norma de grau superior não tem como prever todas as

[495] MIRANDA, Jorge. Teoria da Constituição. Editora Almedina, 2020. Páginas 11 e 12.

suas formas de execução, deixando uma certa discricionariedade para o órgão competente de criar a norma inferior (individualizadora) e, utilizando o mesmo raciocínio, a norma inferior também deixa uma certa discricionariedade para o órgão julgador, que, dentro dos limites da norma, pode escolher a melhor forma de aplicação desta no caso concreto, o que configura à sentença judicial uma função constitutiva do Direito, para além da mera função declarativa. Seria uma interpretação "autêntica", no sentido de que cria o Direito positivo para o caso concreto. Assim, constrói-se uma concatenação de ponta a ponta entre a Constituição até as sentenças judiciais, sendo o fundamento último de validade de tudo a norma fundamental - teoria da interpretação jurídica conforme a Constituição.

Kelsen contesta a interpretação histórica, teleológica e sistemática. O ponto de partida de Kelsen na fundamentação da autonomia metodológica da ciência do Direito é a distinção entre juízos de ser e juízos de dever ser. A ciência do Direito não estaria vinculada com a conduta efetiva do homem, pois não seria uma ciência de factos, pelo contrário, teria relação com as normas que deveriam ser estruturadas dentro de um sistema que teria uma norma fundamental como bússola, que validava toda a estrutura e, por isso mesmo, não seria uma norma posta, mas pressuposta pela ciência do Direito, que deveria ser livre de interesses, paixões ou preconceitos políticos, bem como ser desvinculada da ideia de justiça, por considerar que os valores são variáveis e incompatíveis com um conceito universal de Direito.

O contributo de Kelsen para a "autonomia" do magistrado através da interpretação é inquestionável, mesmo que depois sua teoria da interpretação viesse a ser alvo de críticas, dando margem à outras metodologias, como as teorias de Dworkin e Alexy, fundamentos teóricos do "neoconstitucionalismo" brasileiro (Oliveira, Ana Carolina Borges de, 2019).

Ronald Dworkin, ao desenvolver uma teoria crítica ao positivismo jurídico, aduz que ao lado das regras, há os princípios, que se diferenciam com relação ao seu peso ou sua importância. Dworkin considera que, nos casos complexos, para os quais o juiz não consiga identificar uma regra jurídica aplicável, resolve-se a falta de fundamentação pelos princípios, que seriam o conjunto de padrões que não são regras e que deve ser observado porque é uma exigência de justiça ou equidade

ou alguma outra dimensão da moralidade. (Dworkin, Ronald, O império do direito, 2010, *apud* Oliveira, Ana Carolina Borges de Oliveira, 2019).

Para Dworkin, considerando que em uma sociedade há vários pontos de vista, os juízes só podem invocar princípios que moralmente justificam compromissos já estabelecidos pela sociedade, pois os princípios são extraídos a partir de uma reconstrução dos valores morais que animam a prática jurídica. Na sua obra O Império do Direito, ele defende a aproximação do direito à moral, através dos princípios, na prática judiciária.

Ele considera que nem sempre é o Legislativo quem cria, traça ou delimita as leis, mas sim, o Judiciário, por isso clama pelo compromisso do juiz que deve julgar como se estivesse escrevendo mais uma página de um mesmo romance, mantendo a integridade do direito, que deve ser interpretado como um todo, sendo o princípio o caminho mais adequado para se chegar a uma sentença justa.

Para Alexy, 2015, p. 261, "*Regras são normas que, cumpridas determinadas condições, comandam, proíbem ou permitem algo de forma definitiva ou atribuem poder para algo de forma definitiva.*" São comandos definitivos que se aplicam pela subsunção. Já os princípios são "comandos de otimização", pois determinam que algo seja realizado na maior medida possível em relação às possibilidades fáticas e jurídicas, que determinam o grau de seu cumprimento.

Não é raro que, para uma mesma questão jurídica, exista mais de uma solução jurídica e, para ajudar o magistrado, a teoria da argumentação jurídica de Alexy pode ser utilizada, no sentido de esse pensador considerar que a proposição normativa escolhida deve ser a que possa se fazer acompanhar das melhores razões, ou seja, deve ser a melhor justificada racionalmente.

Cria-se, assim, o discurso jurídico a partir da justificação de um caso especial, que se expressa no julgamento jurídico. A justificação tem dois aspetos: o interno, que se relaciona às premissas utilizadas (ocorre quando a estrutura argumentativa é organizada segundo as estruturas formais das regras ou dos princípios); e o externo, que se relaciona à correção de tais premissas, ou seja, é a fase de justificação das premissas, quando as premissas elencadas na etapa anterior serão fundamentadas. É na justificação externa que a relação entre facto e norma é completada. (GEREMBERG, 2006).

Para se chegar na justificação externa, passa-se pela argumentação empírica, que decorre da observação das especificidades dos factos do caso;

percorre a argumentação dogmática que se baseia na visão do Direito como um sistema coerente fundamentado por meio de razões gerais; também se leva em conta os precedentes como método de interpretação e a analogia, para suprir lacunas.

Para a efetivação da supremacia da constituição, o papel do Poder Judicial, mais precisamente, dos Tribunais Constitucionais, é de suma importância e, quando se aborda esse tema, há de se reconhecer a importância de Hans Kelsen.

Apesar de não ter inventado o Tribunal Constitucional, Hans Kelsen teve grande influência na consolidação do controlo abstrato das leis através em oposição ao modelo norte americano. É certo que a Suprema Corte Americana deu visibilidade ao Poder Judicial, que se tornou, de facto, um Poder da República que, para se fortalecer, teve de deixar cair a máscara da neutralidade, reivindicando o poder de controlar a legitimidade constitucional das leis como poder implícito na função jurisdicional, poder que se consolidou nos Estados Unidos da América após 1883, gerando críticas do tipo "goveno de juízes".

Mas para Kelsen, o controlo difuso (modelo norte-americano) gerava insegurança jurídica porque resolvia o problema apenas no caso concreto, não conferindo unidade ao sistema. Assim, a solução era o controlo concentrado por meio de um órgão com competência primordial de anular leis inconstitucionais, decisões que teriam efeito *ex nunc* e *erga omnis* (atingiria a todos os órgãos do Estado e aos cidadãos em geral).

Diante do novo modelo político que estava a surgir na Áustria após a primeira guerra mundial, que previa a transição democrática e federal do antigo império, o antigo Tribunal Imperial foi transformado num verdadeiro Tribunal Constitucional, sendo este usado como parte integrante de um desenho político mais amplo que previa uma subordinação clara e precisa das regiões ao Centro, numa forma de manter o controlo político.

Assim, em 1 de outubro de 1920 foi aprovada a Constituição Federal da Áustria, que introduziu na Europa a figura do Tribunal Constitucional, sendo Kelsen nomeado magistrado e relator desse Tribunal. Ele considerava que a justiça constitucional era uma afirmação do princípio da separação de poderes, pois a manutenção da República democrática dependia da repartição do exercício do

poder entre diferentes órgãos "*no tanto para aislarlos recíprocamente cuanto para permitir un control recíprocos de uno sobre otros*."[496]

Após a segunda guerra mundial, Itália (1947), Alemanha (1949) e França (1958) promulgaram novas constituições, confiando a Tribunais Constitucionais proteção contra a legislação ordinária. Após instituírem suas respetivas democracias, Portugal (1982) e Espanha (1978) também instituíram seus Tribunais Constitucionais.

A revisão abstrata pode ser o único tipo estabelecida (como na França, antes da reforma de 2008), ou pode ser combinado com uma revisão concreta (como na Áustria, Bélgica, Alemanha, Itália, Portugal, Espanha e França após a reforma de 2008).[497]

No Brasil, o Supremo Tribunal Federal surgiu com inspiração na Suprema Corte Norte-americana, com o controle difuso de constitucionalidade das leis (art. 59, § 1º, b, Constituição de 1891), mas, posteriormente, foi agregado ao ordenamento constitucional brasileiro o controle de constitucionalidade concentrado, inspirado no modelo europeu.

3. Do Ativismo Judicial

É evidente a crescente judicialização da política e politização da justiça, fato que vem desencadeando uma "crise" no Poder Judicial.

Segundo Brito, Wladimir, 2019,[498] o Poder Judicial deriva, assim como os Poderes Legislativo e Executivo, do Poder Político, mas foi nadificado para ter uma aparência de apolítico, ao contrário dos outros dois poderes, que são explicitamente políticos. Ao ser negativado/nulificado em relação aos outros poderes, o Poder Judicial ganhou força para exercer sua função, qual seja, assegurar o respeito pela lei (vigiar e aferir a conformidade prática do exercício do Poder Político com a ordem jurídica a fim de garantir o respeito por essa ordem e pelo poder soberano do povo).

Contudo, o Poder Judicial, mesmo qualificado como nulo, não perde sua essência de Poder Político, do qual deriva. Para esse autor, o Poder Judicial tem que

---

[496] Kelsen, Hans. Escritos sobre Justicia constitucional. Presentación de Manuel Atienza. Traducción de Juan Luis Requejo Pagés. Colección Clássicos del Pensamiento. Tecnos. Página 189.

[497] Comella, Victor Ferreres. Constitutional Cousts Democratic Values – A European Perspective. Yale University Press, 2009.

[498] Brito, Wladimir - Teoria Geral do Processo

se despir da aparência de poder nulo e invisível, roupagem que lhe foi dada por Montesquieu, bem como do conceito de Juizrobôt do positivismo, para ganhar uma nova roupagem, assumindo sua natureza política e seu papel ativo em paridade com os poderes Legislativo e Executivo.

A atual Constituição da República Federativa do Brasil, de 1988, foi promulgada após um período de ditadura, por isso visava a retomada do Estado Democrático de Direito. Além da influência do constitucionalismo norte-americano, teve influência da Constituição da República Portuguesa de 1976, que também foi posterior a uma ditadura.

Houve discussão se o sistema de governo seria o parlamentarismo ou o presidencialismo, pois buscava-se instrumentos mais efetivos de controlo sobre o Poder Executivo e o fortalecimento do Poder Legislativo, mas prevaleceu o sistema presidencialismo, flexibilizado, porque o Presidente da República, como no Parlamentarismo, necessita de uma maioria governista no Congresso Nacional, o que não é fácil, primeiro porque há uma pluralidade de partidos políticos (segundo o Tribunal Superior Eleitoral, há 32 partidos políticos registados no Brasil - https://www.tse.jus.br/partidos/partidos-registrados-no-tse/registrados-no-tse acessado em 29/12/2022). Outro fator é que o Brasil é um país continental com grande diversidade socioeconômica entre as regiões, o que dificulta uma hegemonia ideológica em razão do pluralismo de valores, diversidade que se reflete na representatividade do povo através dos deputados eleitos. (Abranches, 1988).

Assim, a formação de uma coalização para apoiar o Poder Executivo não é tarefa fácil, havendo uma tendência de, no sistema político, haver conflito entre o Executivo e o Legislativo, sendo, o Poder Judicial, chamado a resolver esses conflitos, ocorrendo a judicialização da política, que assim é descrita por Nascimento, Ricardo de Castro, 2017, acessado em 20/12/2022 (https://sapientia.pucsp.br/handle/handle/19760):

> *Após a Constituição de 1988, a dinâmica da divisão de poderes tem evidenciado, ao lado do Presidencialismo de Coalizão, a ascensão do Judiciário, que passou a atuar em campos anteriormente reservados aos demais poderes políticos. Tal fenômeno tem sido conhecido como a judicialização da política.*

Com esse novo papel, o Poder Judicial evidencia sua natureza política. Nesse sentido, CAMPOS, Carlos Alexandre de Azevedo. Dimensões do ativismo judicial do STF, p, 28, acessado em 29/12/2022 (https://www.bdtd.uerj.br:8443/handle/1/9555):

> *"Com essas mudanças, verificadas a partir da Constituição de 1988, o Supremo elevou o padrão de interação como os Poderes Executivo e Legislativo: ele não é mais um simples coadjuvante, mas sim, participante ativo na formação de políticas públicas e na condução do processo democrático brasileiro. Isso tem implicado importante alteração da dinâmica de nosso arranjo institucional, se comparado ao padrão histórico: ainda temos um Poder Executivo – o federal – protagonista e centralizador; o Legislativo – nos três níveis federativos – sofrendo constantes crises funcionais e déficits de confiança popular, mas o Supremo Tribunal Federal, antes uma instituição distante dos grandes temas políticos e sociais e acostumada a submeter a Executivos hipertrofiados, alcançou, de forma gradual, máxime por meio do controle de constitucionalidade das leis, patamar de relevância e autoridade político-normativa absolutamente inédito em sua história (...)".*

Segundo Barroso, 2016, p. 387, a judicialização da política "*é um fato, uma circunstância do desenho institucional brasileiro. Já o ativismo é uma atitude, a escolha de um modo específico e proativo de interpretar a Constituição, expandindo o seu sentido e alcance*", ou seja, é uma forma de fortalecer a Constituição construindo, inclusive, regras específicas de conduta a partir de enunciados vagos (princípios, conceitos jurídicos indeterminados).

Essa nova dimensão de interpretação pode ser sistematizada em quatro principais comportamentos decisórios: (I) interpretação e aplicação das normas constitucionais; (II) interpretação conforme a constituição e declaração de nulidade parcial; (III) controlo da omissão legislativa inconstitucional; (IV) decisões maximalistas (Campos, Carlos Alexandre de Azevedo, Dimensões do ativismo judicial no Supremo Tribunal Federal, 2012).

O modelo "neoconstitucional" nasceu das propostas teóricas de Dworkin e Alexy, apesar das divergências entre as suas teorias. Eles desenvolveram suas respectivas teorias após a Segunda Guerra Mundial, daí a força dos princípios, mas, enquanto Dworkin teve por inspiração a jurisprudência da Suprema Corte norte-americana, Alexy teve por base a jurisprudência do Tribunal Constitucional Alemão.

Conceituando "neoconstitucionalismo", Galvão, Jorge Octávio Lavocat, 2014, p. 59, aduz ser:

> *"uma interpretação da prática jurídica a partir da perspectiva dos juízes, em que a Constituição – editada após o restabelecimento do regime democrático – é tida como uma norma substantiva, composta primariamente de princípios, exigindo do intérprete o manuseio de técnicas especiais, notadamente a ponderação."*

Na Lei de Introdução às normas do Direito Brasileiro há a determinação do Poder Judicial utilizar os princípios gerais do Direito como forma de suprir lacunas (Decreto-Lei nº 4.657, de 4 de setembro de 1942):

> *Art. 4o Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito.*

Observa-se a permissão expressa da utilização de princípios pelos tribunais, que os utiliza não só para suprir omissões, mas também como método de justificação, interpretação, aplicação ou não aplicação das regras, o que exige uma decisão bem fundamentada a fim de lhe conferir validade conforme as leis, princípios e valores, dentro de uma unidade sistêmica que garanta a integridade do direito.

Para Barroso, 2007, o efeito expansivo das normas constitucionais sobre o ordenamento jurídico pode levar a colisões de normas constitucionais, exigindo a ponderação que leva à argumentação, ao controle da racionalidade das decisões proferidas, mediante ponderações nos casos difíceis, que são aqueles que comportam mais de uma solução possível e razoável.

4. Interpretação

Interpretar é uma atividade de mediação pela qual o intérprete traz à compreensão o sentido de um texto que se lhe torna problemático. O texto da lei pode se tornar problemático devido à utilização de conceitos flexíveis, não definidos na lei ou cujas definições sejam incompletas ou quando uma mesma expressão é utilizada em diferentes leis com sentidos diversos. A necessidade de interpretação também pode decorrer de um conflito aparente de normas ou de um concurso de normas. Interpretação é "desentranhamento", difusão e exposição do sentido disposto no texto, mas, de certo modo, ainda oculto. (LARENZ, 2014).

Savigny, no início do século XIX, defendia, na teoria do método do Sistema, a combinação de métodos interpretativos. Para ele, o intérprete precisa "se *colocar*

na posição do legislador e deixar que se formem, por esse artifício, os respectivos ditames" e para isso precisa de três elementos: um elemento lógico (significado de cada texto para o conjunto), um elemento gramatical (particularidades de cada texto) e um elemento histórico o (circunstâncias concretas do aparecimento da lei) - Savigny, 1802 *apud* Larenz, 2014.

Nesses primeiros estudos, Savigny rejeita tanto a interpretação extensiva quanto a restritiva ao afirmar que uma interpretação ampliadora ou extensiva da letra da lei é uma criação artificial do intérprete. Rejeita igualmente a interpretação teleológica, dizendo que o juiz deve ater-se ao que as palavras da lei preceituam, segundo o seu sentido gramatical e lógico, dentro do contexto sistemático porque o magistrado não tem de aperfeiçoar a lei de modo criativo, pois o aperfeiçoamento da lei deve ser obra do legislador, não do intérprete.

Vale ressaltar que essas ideias foram profundamente alteradas quando Savigny passou a considerar como fonte originária do Direito a comum convicção jurídica do povo ao invés a lei, fato que ocorreu pela primeira vez na sua obra "Sobre a vocação do nosso tempo para a ciência da legislação", onde afirma que a lei não nasce de uma dedução lógica, mas sim das típicas formas de conduta que são observadas pelo conjunto dos cidadãos, ou seja, as próprias relações da vida são reconhecidas como típicas do ponto de vista do Direito e estas relações de vida constituem-se nos 'institutos jurídicos', que estão na origem e na fundamentação do Direito. Não são as normas que produzem os institutos jurídicos, pelo contrário, mas é impossível, através das normas, expor esses institutos jurídicos na sua integralidade, ou seja, a lei mostra apenas um segmento deles.

Na segunda metade do século XIX se formaram duas teorias sobre o escopo da interpretação da lei: a teoria subjectivista ou teoria da vontade, e a teoria objectivista ou teoria da interpretação imanente à lei.

Para Karl Larenz, 2014, p.446, a teoria subjetivista considera escopo da interpretação a indagação da vontade histórico-psicológica do legislador. "*A verdade da teoria subjectivista é que a lei jurídica, ao invés da lei natural, é feita por homens e para homens, é expressão de uma vontade dirigida à criação de uma ordem tanto quanto possível justa e adequada às necessidades da sociedade.*"e a teoria objetivista considera escopo da interpretação a exploração do sentido que é inerente à própria lei. Para o autor acima citado, "*A verdade da teoria objectivista*

é que uma lei, logo que seja aplicada, irradia uma acção que lhe é peculiar, que transcende aquilo que o legislador tinha intentado."

Este autor conclui que a teoria subjetivista não pode viver sem arrimo à teoria objetivista porque, para descobrir o sentido da lei é necessário conhecer qual problema jurídico ela visava solucionar, levando-se em conta o contexto político, social e cultural da época (histórico) que lhe são subjacentes, mas, com o decurso do tempo, algumas questões vão perdendo a relevância, dando lugar à outras questões que precisam ser resolvidas por esta mesma lei, que deve ser "reinterpretada", sem dispor do seu sentido normativo original. A "nova" interpretação, para continuar a ser interpretação, tem que manter-se no sentido literal e histórico da lei, o que não impede sua adaptação ao tempo, mesmo que para isso seja preciso uma interpretação "extensiva" ou "restritiva" para manter o escopo da lei, sob pena dela se tornar inaplicável.

> *Se uma norma jurídica é interpretada hoje de modo diverso daquele da sua entrada em vigor há 30 anos, tal está justificado pela sua estrutura histórica temporal. As normas do Direito irradiam o efeito adequado ao seu sentido, enquanto e na medida em que estejam em sintonia com o seu tempo.*" Husserl, Gerhart, Recht und Zeit, p. 26 *apud* Larenz, Karl, Metodologia da Ciência do Direito, p. 448.

Da mesma forma que o legislador precisa ter sempre presente "a convicção jurídica do povo" ao estabelecer a lei *in abstrato*, o aplicador da lei precisa reestabelecer a ligação entre esta "convicção", que é a fonte da lei, e a própria lei, que não consegue abrangê-la na integralidade, e o faz através da interpretação.

Ao interpretar determinado termo ou determinada proposição jurídica, o juiz deve fazê-lo de maneira que a sua interpretação possa ser efetiva para todos os outros casos similares, sob pena de contrariar o postulado da justiça de que os casos iguais devem ser tratados de igual modo, assim como com a segurança jurídica a que a lei aspira. Assim, a interpretação não deve ser deixada ao arbítrio do intérprete e, para evitar este tipo de arbitrariedade, é preciso ter critérios, que não são diferentes métodos de interpretação que o julgador pode escolher arbitrariamente, mas sim, pontos de vista diretivos que se relacionam.

4.1 - Critérios de Interpretação

4.1.1 - O Sentido Literal

O sentido literal constitui o ponto de partida e, ao mesmo tempo, o limite da interpretação. Primeiramente é preciso extrair o significado das palavras no uso linguístico geral porque quem quer dizer algo usa as palavras no sentido em que comummente são entendidas. Contudo, deve-se considerar que o legislador parte do uso linguístico do seu tempo, sob pena de falsear a intenção do legislador se for considerado o uso linguístico do tempo actual quando uma lei antiga é aplicada.

Todavia, o sentido literal não é inequívoco porque uma palavra pode ter mais de um significado, sendo necessário analisar o contexto. "Trata-se aí do processo de olhar para a frente e para trás, do esclarecimento recíproco, que é conhecido pelo nome de "círculo hermenêutico" (p. 452).

Mas o sentido literal também é o limite da interpretação porque uma interpretação fora do sentido literal possível não é interpretação, mas sim, modificação de sentido.

4.1.2 - O Contexto Significativo da Lei

É imprescindível, para compreender o significado específico e um termo ou frase, aferir o contexto do texto como um todo porque a frase ou termo é parte e pertence a uma regulação. Entre várias interpretações possíveis de uma disposição segundo o sentido literal, deve prevalecer a que propicia uma concordância material com outra disposição dentro do mesmo sistema conceptual.

4.1.3 - Intenção Reguladora, Fins e Ideias Normativas do Legislador Histórico

Mas sempre que o sentido literal possível e o contexto significativo da lei e a sistemática conceptual que lhe é subjacente deixarem margem à diferentes interpretações, deve prevalecer a que melhor se ajusta à intenção do legislador e ao escopo da norma em causa, numa análise histórico-teleológica.

Para aferir qual foi a intenção reguladora do legislador e as decisões valorativas por ele encontradas o elemento histórico é imprescindível e, nesse sentido, podem ser fontes dessa intenção os projetos de lei, os pareceres das assessorias legislativas, as exposições de motivos as atas das sessões parlamentares etc.

Interpretação teleológica quer dizer interpretação de acordo com os fins cognoscíveis e as ideias fundamentais de uma regulação. (p. 468). Apesar de ter ciência dos fins que servem de base a uma regulação, muitas vezes o intérprete se depara com situações não previstas originalmente pelo legislador e então, a interpretação terá que extrapolar a "vontade do legislador".

4.1.4 - Critérios Teleológico-Objetivos

Para encontrar a "vontade do legislador" o julgador tem que "acreditar" que ele almejava atingir os fins objetivos do Direito através da lei, ou seja, tem que se nortear pelos princípios ético-jurídicos que precedem a regulação, sendo este o caminho para a resolução justa dos litígios.

4.1.5 - O Preceito da Interpretação Conforme à Constituição

Entre os princípios ético-jurídicos a ser considerados, devem prevalecer os direitos fundamentais da Constituição, ou seja, a prevalência da dignidade da pessoa humana, que é fundamento das Constituições dos Estados signatários da Declaração Universal dos Direitos do Homem.

Uma lei só deve ser declarada inconstitucional se aquela interpretação inconstitucional foi a única possível de acordo com todos os métodos tradicionais. Dentre os vários critérios de interpretação, deve prevalecer aquele que melhor concorde com os princípios da Constituição, respeitando os limites que resultam do sentido literal possível e do contexto significativo da norma, o que não impede uma interpretação restritiva ou extensiva. O importante é atentar-se ao escopo da norma dentro dos princípios constitucionais. A concretização dos princípios é tarefa tanto do legislador quanto da jurisprudência. Segundo Larenz, p. 482

> *"onde o princípio deixe em aberto diferentes possibilidades de concretização, os tribunais estão vinculados à escolhida pelo legislador ordinário, não lhes sendo, portanto, lícito substituí-la por outra – porventura, por via de uma interpretação "conforme à Constituição""*

Só quando a lei não representar a concretização do princípio, é que ela deve ser declarada inconstitucional.

5. Direitos Fundamentais Sociais

Segundo Jorge Bacelar Gouveia[499], quando se fala em direitos fundamentais, a Constituição da República Portuguesa não os conceituou, mas os consagrou através de princípios gerais, que são tipos abertos que conversam entre si. Essa abertura é importante para que a Constituição possa se adaptar às mudanças sociais manifestadas através do processo político da comunidade, mas resguardando os seus princípios fundamentais, e, assim, cumprir sua função integradora em sociedades multifacetadas.

Essa flexibilização se dá, para além da revisão constitucional, tanto pelo legislador (abertura vertical), quanto pela interpretação que os juristas dão sobre as decorrências ou implicações dos princípios "abertos" (abertura horizontal). Percebe-se, então, que o processo hermenêutico é uma forma de alargar o catálogo dos direitos fundamentais, de onde se pode extrair direitos fundamentais implícitos pela interpretação extensiva das fontes constitucionais, inclusivamente fontes externas, como a Declaração Universal dos Direitos do Homem, criando "direitos fundamentais atípicos".

Contudo, até onde pode ir esse processo hermenêutico?

Jorge Bacelar Gouveia considera que há diferença de eficácia entre os direitos fundamentais pelo facto dos direitos, liberdades e garantias versarem sobre normas precetivas (de eficácia imediata) e os direitos econômicos, sociais e culturais versarem sobre normas programáticas (cuja concretização depende da discricionariedade do legislador), isso porque há previsão expressa, no artigo 18º da Constituição da República Portuguesa, de aplicabilidade direta e vinculação das entidades públicas e privadas apenas para os direitos, liberdades e garantias. Disso se conclui que, em relação aos direitos sociais, sua aplicabilidade depende de lei e/ou de políticas públicas, o que, num primeiro momento, inibe a atuação do Poder Judicial.

No Brasil, como não há essa expressa diferenciação do regime de proteção entre os direitos sociais e os direitos, liberdades e garantia, a discussão versa sobre serem os direitos sociais reais direitos fundamentais.

Ingo Wolfgang Sarlet considera que, ao analisar a Constituição, tem de se aferir a finalidade da norma, porque nem todas são de direitos fundamentais. Para ser direito fundamental em sentido material, tem de ser universal dentro de uma

[499] Gouveia, Jorge Bacelar. Manual de Direito Constitucional. II – Direito Constitucional Português. 6ª edição, 2016.

parâmetro ético-moral mínimo, ou seja, os direitos fundamentais são pré-originários, que o Estado não concede, mas apenas reconhece, por isso geralmente são reconhecidos internacionalmente, através de tratados, como a Declaração Universal dos Direitos do Homem.

O desenvolvimento dos direitos sociais como *standards* mínimos para a vida permite concluir que eles são meios para se garantir a dignidade humana, o que lhe confere *status* de direito fundamental. Sendo assim, é cláusula pétrea, de aplicação imediata e vincula as entidades públicas e privadas, prescindindo de declaração nesse sentido. Mesmo sendo diretamente aplicável, a eficácia de um direito fundamental pode ser limitada.

O Supremo Tribunal Federal vem reconhecendo que os direitos sociais são direitos fundamentais, gerando a consequência de eles terem aplicabilidade imediata. Ressalta-se que isso não significa que todos os direitos sociais devam ser pronta e imediatamente promovidos sem limites, pois não são absolutos. Mas, por outro lado, significa que eles não estão na esfera de **discricionariedade absoluta** do Legislativo e/ou Executivo, apesar de estarem intimamente relacionados a decisões políticas sobre os meios de sua implementação.

Entre as funções institucionais do Supremo Tribunal Federal não está a atribuição de formular políticas públicas, pois, nesse domínio, o encargo reside, primariamente, nos Poderes Legislativo e Executivo.[500] Mas excecionalmente o Poder Judicial pode assumir essa incumbência se e quando os órgãos estatais competentes, por descumprirem os encargos político-jurídicos que sobre eles incidem, vierem a comprometer, com tal comportamento, a eficácia e a integridade de direitos individuais e/ou coletivos impregnados de estatura constitucional, ainda que derivados de cláusulas revestidas de conteúdo programático, que, conforme entendimento do Supremo Tribunal Federal, não é mera promessa inconsequente porque representa expectativa do poder constituinte e do povo que ele representa. Por isso, o incumprimento injustificável do poder-dever de agir configura infidelidade governamental.

É um poder-dever: dever que advém de um comando constitucional; em outras palavras: do poder constituinte; em outras palavras: do Estado Democrático

[500] JOSÉ CARLOS VIEIRA DE ANDRADE, "Os Direitos Fundamentais na Constituição Portuguesa de 1976", p. 207, item n. 05, 1987, Almedina, Coimbra).

de Direito; em outras palavras: da vontade do povo. Mas o cumprimento desse dever é condicionado à "reserva do possível", diante da onerosidade para a efetivação e implementação dos direitos econômicos, sociais e culturais. Todo direito fundamental tem aplicabilidade imediata, mas isso não significa efetividade total como se fosse um direito subjetivo do cidadão. A densidade dessa efetividade depende de políticas públicas, dentro da reserva do possível, para uma efetivação gradual.

Assim, o intérprete só pode determinar a efetivação e implementação de políticas públicas pelo Estado se restar configurado o abuso, o que exige do julgador ponderação e razoabilidade.

6. Da Omissão Legislativa

Segundo o Supremo Tribunal Federal, a omissão do Estado – que deixa de cumprir, em maior ou em menor extensão, a imposição ditada pelo texto constitucional, qualifica-se como comportamento revestido de intensa gravidade político-jurídica, eis que, mediante inércia, o Poder Público também desrespeita a Constituição, também ofende direitos que nela se fundam e também impede, por ausência (ou insuficiência) de medidas concretizadoras, a própria aplicabilidade dos postulados da Lei Fundamental.

A ação direta de inconstitucionalidade por omissão tem por objetivo provocar a jurisdicional que, expressamente autorizada e atribuída ao Supremo Tribunal Federal pela Constituição, visa impedir o desprestígio da Lei Fundamental e proteger princípios, direitos e garantias nela proclamados.

Conclusão

A crescente autonomia do processo hermenêutico vem dando visibilidade ao direito constitucional adaptável ao sinal dos tempos e, consequentemente, ao problema da legitimidade da justiça constitucional, no que se traduz na expressão "ativismo judicial".

Segundo Barroso, Luís Roberto,[501] o intérprete judicial, ao ponderar os fatos, as normas e os valores, faz uma escolha política ao decidir qual solução aplicar entre as possíveis, completando, assim, "o trabalho do legislador".

A interpretação e a argumentação se relacionam, já que ao escolher um critério de interpretação no lugar de outro, o magistrado já está escolhendo os argumentos favoráveis e contrários que irá utilizar. Contudo, a interpretação não pode ser o argumento utilizado pelo juiz para manipular a lei de acordo com as suas convicções pessoais, o que põe em risco o Estado de Direito. Percebe-se, então, a necessidade da ética e da hermenêutica na formação da decisão judicial justa nos limites do Direito.

No caso do Presidente Lula, narrado no início deste trabalho, o Supremo Tribunal Federal declarou a constitucionalidade de um dispositivo legal, dando máxima efetividade ao princípio constitucional da presunção do estado de inocência, mitigando o princípio da segurança jurídica.

Votaram[502] pela manutenção da interpretação de que a execução da pena antes do trânsito em julgado, desde que a condenação tenha sido ratificada em segunda instância, não lesa o princípio da presunção de inocência (o que manteria o Senhor Lula preso), os seguintes ministros: Alexandre de Moraes (indicado pelo Presidente Michel Temer – direita), Edson Fachin (indicado pela Presidente Dilma Rousseff – esquerda), Luís Roberto Barroso (indicado pela Presidente Dilma Rousseff – esquerda), Luiz Fux (indicado pela Presidente Dilma Rousseff – esquerda), Cármen Lúcia (indicada pelo Presidente Luiz Inácio Lula da Silva, esquerda). Ou seja, apesar de 4 dos 5 ministros que votaram pela execução provisória da pena terem sido indicados pelo Partido dos Trabalhados (partido do político Luiz Inácio Lula da Silva), eles votaram contra os interesses do Lula, não havendo indícios de parcialidade.

Os outros seis ministros que votaram pela constitucionalidade do artigo do Código de Processo Penal que condicionava a prisão ao trânsito em julgado da condenação (o que ensejaria a soltura de Lula) foram: Marco Aurélio (indicado pelo Presidente Fernando Color de Mello, que era seu primo e político da direita), Rosa

[501] BARROSO, Luís Roberto. Neoconstitucionalismo e constitucionalização do direito (O triunfo tardio do direito constitucional no Brasil). In: Temas de Direito Constitucional. Tomo IV. Op. cit., p. 72.

[502] https://www.conjur.com.br/wp-content/uploads/2023/09/adc-43-stf-publica-acordaos-julgamento.pdf

Weber (indicada pela Presidente Dilma Rousseff – esquerda), Ricardo Lewandowski (indicado pelo Presidente Luiz Inácio Lula da Silva, esquerda), Gilmar Mendes (indicado pelo Presidente Fernando Henrique Cardoso – direita), Celso de Melo (indicado pelo Presidente José Sarney – direita) e Dias Toffoli (indicado pelo Presidente Luiz Inácio Lula da Silva, esquerda).

Formalmente, esse órgão não extrapolou sua competência e, se houve "interesse político" por trás dessa decisão, apesar das evidentes repercussões, não se pode provar, até porque não foi uma decisão unânime, havendo 05 votos vencidos contra 6 e nem todos os ministros indicados pelo próprio Presidente Lula votaram em seu favor.

Ressalta-se que o fato de uma decisão colegiada não ser unânime não significa que um ou outro magistrado agiu com má-fé. Quando isso ocorre geralmente estão em causa princípios que, naquele caso, estão em conflito, o que exige um juízo de ponderação. Mas como não existe uma fórmula matemática para fazer esse juízo de ponderação, bem como há uma igualdade hierárquica entre os princípios, cada magistrado irá julgar conforme seus valores éticos e morais.

Evidencia-se, nesse ponto, a importância da argumentação jurídica utilizada na fundamentação da decisão, a fim de justificar a escolha de determinada norma em detrimento de outra, ou a escolha desse ou daquele critério de interpretação. É a qualidade desses argumentos que acaba por legitimar a decisão judicial.

O fenômeno da constitucionalização do Direito deu grande visibilidade aos Tribunais Constitucionais ao exercerem o controlo da constitucionalidade das leis, onde acabam por agir como "legisladores negativos e positivos". Pode-se constatar a superação progressiva do dogma kelseniano do juiz constitucional apenas como legislador negativo com o avanço da figura desse juiz também como legislador positivo, criador de normas gerais ao interpretá-las, o que evidencia o aspeto político do Poder Judicial. Nesse sentido completa Brito, Wladimir, 2019, p. 8e6:

> *"a Justiça Constitucional, por essa via legislativa e, ainda, pela do controlo dos conflitos entre órgãos do poder político, da constitucionalidade das instituições e dos processo políticos, acaba por ser um órgão que exerce uma função política de controlo do próprio poder político."*

Superada a conceção de separação de poderes que afasta do Poder Judicial a apreciação de políticas públicas, pois, como guardião da constituição, o

Supremo Tribunal Federal não pode ser conivente com ações ou omissões abusivas dos poderes executivo e legislativo.

Essa intervenção tem que ser razoável, em respeito ao poder discricionário desses poderes. Todavia, dentro de um Estado Democrático de Direito, a discricionariedade dos poderes não pode ser absoluta, sob pena de tirar toda força constitucional de uma norma programática, que, assim como as normas de aplicação imediata, configuram compromissos constitucionais que o Estado assumiu em nome do povo.

Analisando a ADPF 45/2004, onde o STF interferiu na concretização de políticas públicas na área da saúde, observa-se que foi uma conduta pró-ativa, característica do neo-constitucionalismo, cujo núcleo é centrado nos direitos fundamentais consagrados pelo poder constituinte originário ao instituir o Estado Democrático de Direito, e que por isso devem servir como limites jurídico-constitucionais efetivos.

A fundamentação dessa decisão a tornou razoável e, apesar da conotação política, livre de ilegalidade em razão do que estava em causa, pois, num Estado Democrático de Direito, o Poder Executivo não é livre para fazer o que quiser.

O desrespeito à Constituição tanto pode ocorrer mediante ação estatal quanto mediante omissão. A situação de inconstitucionalidade pode derivar de um comportamento ativo do Poder Público, que age ou edita normas em desacordo com o que dispõe a Constituição, mas também pode derivar do facto do Estado deixar de adotar as medidas necessárias à realização concreta dos preceitos da Constituição, em ordem a torná-los efetivos, operantes e exequíveis, abstendo-se, de cumprir o dever de prestação que a Constituição lhe impôs, configurando a inconstitucionalidade por omissão, que pode ser total, quando é nenhuma a providência adotada, ou parcial, quando é insuficiente a medida efetivada pelo Poder Público.

Se tratando de Ação Declaratória de Inconstitucionalidade por Omissão, a própria Constituição impôs ao Supremo Tribunal Federal um limite: apenas declarar a omissão e cientificar o órgão omisso. Por essa razão, quando o STF extrapola esse limite, mesmo com a justificativa de estar dando efetividade à Constituição, há um desrespeito à própria Constituição, seja ao artigo 103, §2º, que impõe esse limite, bem como ao princípio da separação dos poderes, expresso no artigo 2º: *São Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário.*

Contudo, para além de reconhecer a mora constitucional e notificar o órgão competente (que deveria ter legislado), o Supremo Tribunal Federal vêm sanando as omissões determinando como a situação deve ser resolvida até que seja editada lei.

Nesse sentido são, por exemplo, o julgamento da ADO 26/DF, onde esse órgão determinou que:

> *"Até que sobrevenha lei emanada do Congresso Nacional destinada a implementar os mandados de criminalização definidos nos incisos XLI e XLII do art. 5º da Constituição da República, as condutas homofóbicas e transfóbicas, reais ou supostas, que envolvem aversão odiosa à orientação sexual ou à identidade de gênero de alguém, por traduzirem expressões de racismo, compreendido este em sua dimensão social, ajustam-se, por identidade de razão e mediante adequação típica, aos preceitos primários de incriminação definidos na Lei nº 7.716, de 08/01/1989, constituindo, também, na hipótese de homicídio doloso, circunstância que o qualifica, por configurar motivo torpe (Código Penal, art. 121, § 2º, I, "in fine");"* .[503]

A omissão do Poder Legislativo da União seria em relação ao mandamento constitucional que impõe ao Estado o dever de proteção à essencial dignidade das pessoas, a ser efetivado mediante tipificação penal dos atos de discriminação praticados em razão da orientação sexual ou da identidade de gênero das vítimas de tais práticas discriminatórias, nos termos do artigo 5º, incisos XLI e XLII, da Constituição Federal:

> *XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais;*
>
> *XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;*

Todo o fundamento desse acórdão é razoável, pois o STF confere uma interpretação extensiva ao conceito de racismo, que, na nossa sociedade contemporânea, se subsume mais ao sentimento que fundamenta qualquer discriminação do que simplesmente a cor da pele e a proibição constitucional de qualquer tipo de discriminação.

[503] https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754019240

Contudo, a Constituição Federal concede competência exclusiva à União para legislar sobre direito penal[504] e, utilizando a tese da "interpretação conforme", o Supremo Tribunal Federal acabou por criar um tipo penal, que, apesar dele expressamente aduzir que não se trata de analogia, na realidade é, pois ele buscou um tipo penal já existente para suprir uma omissão, o que fere os princípios restritivos do Direito Penal, que é regido, precipuamente, pelo princípio da legalidade, expresso tanto no artigo 5º, inciso XXXIX, da Constituição Federal, quanto no artigo 1º do Código Penal Brasileiro: não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.[505]

Por isso mesmo, houve votos vencidos, no sentido de apenas declarar a omissão, como determina o artigo 103, §2º, da CRFB/88: *Declarada a inconstitucionalidade por omissão de medida para tornar efetiva norma constitucional,* ***será dada ciência ao Poder competente para a adoção das providências necessárias*** *e, em se tratando de órgão administrativo, para fazê-lo em trinta dias.*

Portanto, nesse caso, houve violação ao princípio da separação de poderes.

Bibliografia

ABRANCHES, Sérgio Henrique Hudson de. Presidencialismo de coalização: o dilema institucional brasileiro, Revista de Ciências Sociais, vol. 31, nº 1, p. 5 a 34. Rio de Janeiro: 1988. Acesso digital - http://dados.iesp.uerj.br/artigos/?id=348 acesso em 22/11/2022

ARISTÓTELES, Política, 2ª ed. Trad. Nestor Silveira Chaves, São Paulo: Edipro, 2009.

BARROSO, Luís Roberto. Neoconstitucionalismo e constitucionalização do direito: o triunfo tardio do direito constitucional no Brasil. Biblioteca Digital do Tribunal de Justiça do Distrito Federal, pdf https://bd.tjdft.jus.br/jspui/handle/tjdft/9949 acessado em 08/01/2023

BONAVIDES, Paulo. Curso de Direito Constitucional. 10. Ed. São Paulo: Malheiros, 1988.

[504] Art. 22. Compete privativamente à União legislar sobre:

I - direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho;

[505] https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BOBBIO, Norberto. Locke e o direito natural. Trad. Sérgio Bath. Brasília: Edunb, 1997. Pdf em https://pt.scribd.com/document/346682614/BOBBIO-Norberto-Locke-e-o-Direito-Natural acesso em 15/12/2022

BRASIL. Constituição 1988. Brasília: Senado Federal, 2018, pdf https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm acesso em 10/11/2022

BRITO, Wladimir, Teoria Geral do Processo, Almedia, 2019.

CAMPOS, Carlos Alexandre de Azevedo, Dimensões do ativismo judicial no Supremo Tribunal Federal, Biblioteca Digital de Teses e Dissertações da Universidade Estadual do Rio de Janeiro, Brasil, 2012, pdf http://www.bdtd.uerj.br/handle/1/9555 acessado em 29/12/2022.

CANOTILHO, José Joaquim Gomes, Direito constitucional e teoria da constituição. 7. ed., Coimbra: Almedina, 2003.

GALVÃO, Jorge Octávio Lavocat, O Neoconstitucionalismo e o fim do Estado de Direito, São Paulo: Saraiva, 2014.

GEREMBERG, Alice Leal Wolf, A teoria compreensiva de Robert Alexy: a proposta do 'trialismo', Tese de doutorado apresentada na Puc-Rio. Rio de Janeiro, 2006. Disponível em: < http://www.maxwell.lambda.ele.puc-rio.br/9593/9593_3.PDF>. Acesso em: 22/12/2022.

HOMEM, António Pedro Barbas, O Justo e o Injusto, ed. AAFDL, 2017.

LARENZ, Karl, Metodologia da Ciência do Direito, 7ª ed., Fundação Calouste Gulbenkian, 2014

LOCKE, John, Dois Tratados do Governo Civil, traduzido por Miguel Morgado, Editora Edições 70 Lda, 2015.

LOCKE, John, Dois tratados sobre o governo, Tradução de Júlio Fischer e Introdução de Peter Laslett, São Paulo: Martins Fontes, 1998 (Clássicos) pdf em https://www.academia.edu/40403766/John_Locke_Dois_Tratados_Sobre_o_Governo acesso em 15/12/2022

MARTINS, Ricardo Marcondes, Neoconstitucionalismo, Tomo Direito Administrativo e Constitucional, Edição 1, Abril de 2017, Enciclopédia Jurídica da Pontifícia Universidade Católida de São Paulo, pdf https://enciclopediajuridica.pucsp.br/verbete/134/edicao-1/neoconstitucionalismo acesso em 13/12/2022

MONTESQUIEU, Charles de Secondat, Baron de, 1689-1755 (2000), O Espírito da Leis, Editora Martins Fontes, São Paulo. Pdf em https://edisciplinas.usp.br/pluginfile.php/2963710/mod_resource/content/0/Montesquieu-O-espirito-das-leis_completo.pdf acesso em 15/12/2022 acesso em 17/11/2022

NASCIMENTO, Ricardo de Castro, Divisão de Poderes – Origem, Desenvolvimento e Atualidades, Tese de doutorado apresentada na Pontifícia Universidade de São Paulo, 2017, pdf https://sapientia.pucsp.br/bitstream/handle/19760/2/Ricardo%20de%20Castro%20Nascimento.pdf acesso em 23/11/2022

NOVAES, Adauto, Ética, São Paulo: Companhia das Letras; Secretaria Municipal de Cultura, 1992.

OLIVEIRA, Ana Carolina Borges de, Princípios Jurídicos e Pós-positivismo – A Formação das Decisões Judiciais no Direito Brasileiro, Porto, Editorial Juriá, 2019

PELICIOLI, Ângela Cristina, A atualidade da reflexão da separação de poderes, Revista de Informação Legislativa - Brasília a. 43 n. 169 jan./mar. 2006 https://www12.senado.leg.br/ril/edicoes/43/169/ril_v43_n169_p21.pdf acesso em 16/12/2022

PISKE, Oriana e SARACHO, Antonio Benites, Considerações sobre a Teoria dos freios e contrapesos (Checks and Balances System), revista do TJDF pdf https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2018 acesso em 08/12/2022

Supremo Tribunal Federal - https://www.conjur.com.br/wp-content/uploads/2023/09/adc-43-stf-publica-acordaos-julgamento.pdf

VASCONCELOS, Pedro Carlos Barbosa de. Teoria geral do controlo jurídico do poder público. Lisboa: Edições Cosmos, 1996.

Impugnação de Decisões e a Importância dos Recursos: Garantindo a Justiça e a Correção de Erros no Sistema Legal: Uma Análise à Luz da Teoria Geral do Processo de Wladimir Brito[506]

Nathannael Santiago Alves de Lana

[506] Estudo realizado no âmbito do Mestrado em Direito Judiciário, da Universidade Europeia.

Introdução

Para um melhor entendimento do tema em questão, é fundamental abordar a impugnação de decisões judiciais no contexto jurídico. Como Miguel Teixeira de Sousa[507] salienta, as decisões judiciais são passíveis de contestação por meio de dois principais instrumentos: a reclamação e o recurso. Esta prática é amplamente aceita e tradicional no sistema legal, permitindo que as partes insatisfeitas contestem decisões que considerem injustas ou errôneas. O cerne do assunto envolve a percepção de que, em geral, as decisões judiciais não são irrevogáveis, e a maioria dos sistemas legais concede às partes o direito de questionar aquelas que julgam desfavoráveis, injustas ou ilegais.

Dentro desse contexto, é essencial considerar que, por via de regra, a impugnação no processo judicial depende da iniciativa das partes, ou seja, não ocorre de forma automática por parte do tribunal. As partes envolvidas têm a responsabilidade de solicitar ativamente a revisão das decisões, garantindo, assim, que a impugnação ocorra. Esses meios processuais disponíveis, que incluem a reclamação e o recurso, são acionados pelas partes e desempenham um papel crucial na busca por justiça e na correção de erros de julgamento.

O recurso, um dos principais meios de impugnação, é um instrumento que as partes e o Ministério Público utilizam para solicitar a revisão de decisões judiciais. Normalmente, é empregado quando as partes se sentem prejudicadas pela decisão original e desejam modificá-la. O recurso envolve a revisão ou reavaliação de uma decisão dentro do mesmo processo e relação jurídico-processual, com a possibilidade de alterar a decisão original. Assim, o direito de recorrer é frequentemente exercido por partes que discordam da decisão e desejam contestá-la. No entanto, o Ministério Público, em determinadas situações, também pode agir como custos legis, conforme exigido pela lei, como afirma Ovídio a. baptista da Silva e Fábio Luiz Gomes, "*excluir, ou deixar sem explicação, os recursos interpostos pelo órgão do Ministério Público, que, nos casos e que intervém na causa, como simples custos legis, não poderá ter sido como sucumbente*"[508]

É importante ressaltar que, embora o recurso permita a revisão da decisão, ele não inicia um novo processo. Em vez disso, é uma fase subsequente do mesmo processo, tratada por um tribunal hierarquicamente superior ao tribunal original, com a competência jurídico-processual apropriada, conforme informa Castro Mendes, "*nisto: a reclamação representa um pedido de revisão do problema sobre que incidiu a decisão judicial, revisão feita pelo mesmo órgão Judicial e sobre a mesma situação em face da qual decidiu; o recurso representa um pedido de revisão da legalidade ou ilegalidade da decisão judicial, feita por um órgão judicial*

[507] Miguel Teixeira de Sousa (1997: 369)

[508] Ovídio a. baptista da Silva e Fábio Luiz Gomes (2011: 278).

diferente (superior hierarquicamente) ou em face de argumentos espe-ciais feitos valer"[509]. O duplo grau de jurisdição, que envolve a revisão de casos por uma segunda instância judicial, é um princípio amplamente aceito em sistemas jurídicos. Ele se baseia na ideia de garantir a correção de erros de julgamento e na busca por decisões justas.

No entanto, a Constituição lida indiretamente com o princípio do direito de recorrer, assim entende Amâncio Ferreira, "*havendo uma hierarquia na ordem dos tribunais judiciais, tendo como órgão superior o STJ; e tribu-nais de primeira e de segunda instância, implicitamente se admite que as decisões dos tribunais de primeira instância podem ser impugnadas perante os tribunais de segunda instância e as destes perante o STJ (neste último caso em reconhecimento do triplo grau de jurisdição)*[510]. Ela concede ao legislador ordinário a flexibilidade de decidir se consagra ou não esse princípio, desde que não comprometa o sistema constitucional estabelecido. Assim, a regulamentação dos recursos nos processos civis pode variar, mas não deve restringir excessivamente o direito de recorrer a ponto de eliminá-lo. Dentro desse contexto, o legislador tem a flexibilidade de ampliar ou limitar os recursos em processos civis, respeitando os limites constitucionais, princípios de igualdade e proporcionalidade.

Quanto à natureza jurídica do recurso, a doutrina apresenta duas correntes de pensamento. Alguns, como Marcus Vinicius Rios Gonçalves[511], veem o recurso como um remédio no mesmo processo, enquanto outros o consideram semelhante a uma ação. Ambas as correntes concordam que o recurso é um direito subjetivo público processual, embora sua natureza específica possa variar. Neste contexto, os recursos desempenham um papel fundamental na busca pela justiça e na garantia de que decisões judiciais injustas ou errôneas possam ser contestadas e, se necessário, modificadas.

Esta introdução proporciona uma visão geral dos principais conceitos relacionados à impugnação de decisões judiciais, incluindo a natureza dos recursos, o papel do duplo grau de jurisdição e a flexibilidade constitucional na regulamentação dos recursos nos processos civis. Os próximos tópicos irão aprofundar esses aspectos e fornecer uma compreensão abrangente dos meios de impugnação no contexto jurídico.

Impugnação de Decisões Judiciais

A impugnação de decisões judiciais é um aspecto fundamental no sistema legal, permitindo que as partes insatisfeitas contestem as decisões que consideram injustas ou errôneas.

[509] Castro Mendes (1980: 3)

[510] Fernando amâncio Ferreira (2005: 77).

[511] Cfr. Marcus Vinicius rios Gonçalves (2008: II: 37).

Se tratando da Natureza da Impugnação de Decisões Judiciais a impugnação de decisões judiciais refere-se à capacidade das partes envolvidas em um processo judicial de contestar as decisões emitidas pelo tribunal. Isso é uma prática tradicional em sistemas legais e é amplamente aceito como uma parte fundamental do processo legal, e Miguel Teixeira de Sousa afirma "As decisões judiciais podem ser impugnadas mediante reclamação ou recurso"[512]

Meios de Impugnação: As partes insatisfeitas têm dois principais meios de impugnação de decisões judiciais: reclamação e recurso. A reclamação envolve a revisão da decisão pelo mesmo juiz que a proferiu, enquanto o recurso permite que uma instância judicial hierarquicamente superior revise a decisão, conforme afirma Castro Mendes, "*nisto: a reclamação representa um pedido de revisão do problema sobre que incidiu a decisão judicial, revisão feita pelo mesmo órgão Judicial e sobre a mesma situação em face da qual decidiu; o recurso representa um pedido de revisão da legalidade ou ilegalidade da decisão judicial, feita por um órgão judicial diferente (superior hierarquicamente) ou em face de argumentos espe-ciais feitos valer*"[513].

Iniciativa das Partes: A impugnação de decisões judiciais não ocorre automaticamente. As partes devem tomar a iniciativa de solicitar a revisão da decisão se desejarem contestá-la. Isso significa que as partes têm um papel ativo no processo de impugnação, conforme afirma Wladimir Brito "*Importa finalmente dizer que todas as impugnações dependem da ini-ciativa das partes ou seja nunca são oficiosamente feitas. Têm de ser as par-tes a deduzi-las, pedindo a reapreciação da decisão, estando, portanto, na disponibilidade delas o uso desses meios processuais*"[514].

Com isto podemos verificar que o objetivo do recurso seja um meio de obter uma nova decisão que substitua a decisão original, podendo esta ser modificada, anulada ou revogada. Geralmente, é usado pelas partes que se sentem prejudicadas pela decisão original.

Duplo Grau de Jurisdição: O princípio do duplo grau de jurisdição envolve a revisão de casos por uma segunda instância judicial, o que é fundamental para garantir a correção de erros de julgamento e buscar decisões justas, é o que pontua Amâncio Ferreira, "*havendo uma hierarquia na ordem dos tribunais judiciais, tendo como órgão superior o STJ; e tribu-nais de primeira e de segunda instância, implicitamente se admite que as decisões dos tribunais de primeira instância podem ser impugnadas perante os tribunais de segunda instância e as destes perante o STJ (neste último caso em reconhecimento do triplo grau de jurisdição)*"[515].

Princípio do Direito de Recorrer: A Constituição e a legislação geralmente estabelecem o princípio do direito de recorrer, permitindo que as partes contestem

[512] Miguel Teixeira de Sousa (1997: 369).

[513] Castro Mendes (1980: 3)

[514] Wladimir Brito (2020: 345)

[515] Fernando amâncio Ferreira (2005: 77).

decisões judiciais. No entanto, o legislador tem a flexibilidade de expandir ou limitar os recursos, desde que respeite os limites constitucionais, para que não acabe se restringindo "excessivamente o direito de recorrer consagrado em termos de se poder concluir que os recursos tenham sido efectivamente suprimidos" o que afirma Amâncio Ferreira[516].

Natureza Jurídica do Recurso: A natureza jurídica do recurso é debatida na doutrina, havendo duas correntes de pensamento. Alguns veem o recurso como um remédio dentro do mesmo processo, como Marcus Vinicius rios Gonçalves[517], enquanto outros o consideram semelhante a uma ação, compartilhando a natureza jurídica desta, conforme Miguel Teixeira de Sousa, ao afirmar "As decisões judiciais podem ser impugnadas mediante reclamação ou recurso"[518]

Em resumo, a impugnação de decisões judiciais desempenha um papel vital no sistema legal, garantindo que as partes tenham a capacidade de contestar decisões que consideram injustas ou errôneas. Os meios de impugnação, como a reclamação e o recurso, oferecem às partes uma maneira de buscar uma revisão das decisões judiciais em busca de justiça. O princípio do duplo grau de jurisdição e o direito de recorrer são componentes fundamentais desse sistema, garantindo a correção de erros e o devido processo legal. A natureza jurídica do recurso pode variar dependendo da abordagem doutrinária, mas sua importância na proteção dos direitos das partes é indiscutível.

Meios de Impugnação

Os meios de impugnação, como a reclamação e o recurso, desempenham um papel fundamental no sistema legal, permitindo que as partes contestem decisões judiciais que consideram injustas ou errôneas. Vamos destacar a diferença entre esses dois meios, com ênfase na revisão pela mesma instância judicial e por um órgão judicial superior.

Conforme afirma Castro Mendes, "*nisto: a reclamação representa um pedido de revisão do problema sobre que incidiu a decisão judicial, revisão feita pelo mesmo órgão Judicial e sobre a mesma situação em face da qual decidiu; o recurso representa um pedido de revisão da legalidade ou ilegalidade da decisão judicial, feita por um órgão judicial diferente (superior hierarquicamente) ou em face de argumentos espe-ciais feitos valer*"[519]. Confome podemos conferir a seguir.

Reclamação:

[516] Fernando amâncio Ferreira (2005: 78).

[517] Cfr. Marcus Vinicius rios Gonçalves (2008: II: 37).

[518] Miguel Teixeira de Sousa (1997: 369).

[519] Castro Mendes (1980: 3)

Na reclamação, a revisão da decisão é realizada pelo mesmo juiz que proferiu a decisão original, conforme apresenta Miguel Teixeira de Sousa, "*As decisões judiciais podem ser impugnadas mediante reclamação ou recurso*"[520]

Este meio de impugnação permite que as partes questionem diretamente a decisão perante o mesmo juiz, alegando irregularidades, erros ou injustiças no processo.

Normalmente, a reclamação é usada para contestar atos do juiz que afetam a validade ou legalidade do processo, como decisões interlocutórias ou incidentes processuais.

Recurso:

O recurso envolve a revisão da decisão por um órgão judicial hierarquicamente superior ao tribunal original que emitiu a decisão, pontua Amâncio Ferreira, "*havendo uma hierarquia na ordem dos tribunais judiciais, tendo como órgão superior o STJ; e tribu-nais de primeira e de segunda instância, implicitamente se admite que as decisões dos tribunais de primeira instância podem ser impugnadas perante os tribunais de segunda instância e as destes perante o STJ (neste último caso em reconhecimento do triplo grau de jurisdição)*"[521].

A revisão é realizada por um tribunal de segunda instância ou um tribunal superior, comumente conhecido como tribunal de apelação ou corte suprema.

Geralmente, o recurso é apresentado quando uma das partes envolvidas no caso não concorda com a decisão e busca uma revisão ou uma nova decisão.

O recurso é um mecanismo importante para garantir que decisões judiciais sejam revisadas por uma instância independente, evitando parcialidade ou erros.

Ambos os meios de impugnação requerem a iniciativa das partes, o que significa que as partes insatisfeitas devem solicitar ativamente a revisão da decisão por meio de reclamação ou recurso. A decisão de impugnar uma decisão judicial é uma estratégia legal que as partes utilizam para proteger seus direitos e interesses, diante do apresentado anteriormente.

Além disso, a natureza do recurso envolve a revisão de uma decisão judicial antes que ela se torne definitiva, com o objetivo de obter uma nova decisão que possa modificar, anular ou revogar a decisão original. O duplo grau de jurisdição desempenha um papel importante, garantindo que a revisão de casos seja realizada por uma segunda instância judicial, o que é fundamental para a busca de decisões justas e a correção de erros de julgamento.

Quanto à natureza jurídica do recurso, há debates na doutrina, mas em geral, é considerado um direito subjetivo público processual que as partes têm para contestar uma decisão judicial. Pode ser visto como um meio especial de contestar

[520] Miguel Teixeira de Sousa (1997: 369).

[521] Fernando amâncio Ferreira (2005: 77).

decisões, com características próprias e elementos em comum com uma ação judicial, como interesse, legitimidade e capacidade de agir, conforme já mencionado.

Em resumo, a reclamação e o recurso são os principais meios de impugnação de decisões judiciais, com a principal diferença sendo a autoridade que revisa a decisão, com a reclamação sendo revisada pelo mesmo juiz e o recurso por um órgão judicial superior hierarquicamente. Ambos desempenham um papel fundamental no sistema legal, garantindo a justiça e a correção de erros no processo judicial.

Iniciativa das Partes na Impugnação

Iniciativa das Partes na Impugnação: Em geral, a impugnação de decisões judiciais não ocorre automaticamente pelo tribunal. As partes envolvidas no processo devem solicitar ativamente a revisão da decisão se considerarem que é injusta ou errônea. Portanto, a iniciativa para iniciar uma reclamação ou recurso parte das partes diretamente, não ocorrendo de ofício pelo tribunal. conforme afirma Wladimir Brito *"Importa finalmente dizer que todas as impugnações dependem da ini-ciativa das partes ou seja nunca são oficiosamente feitas. Têm de ser as par-tes a deduzi-las, pedindo a reapreciação da decisão, estando, portanto, na disponibilidade delas o uso desses meios processuais"*[522].

Recurso como Meio de Impugnação: O recurso é um meio de impugnação que permite às partes ou ao Ministério Público pedir a revisão de uma decisão judicial com o objetivo de modificá-la, normalmente quando se sentem prejudicados pela decisão original. É uma etapa subsequente do mesmo processo, tratada por um tribunal hierarquicamente superior com competência jurídico-processual adequada, o quê diz Wladimir Brito "Podemos concluir dizendo que a revista originariamente era um meio de impugnação de decisões, com fundamento na nulidade ou na injus-tiça notória, que não se restringia a questões de direito, por o Tribunal de revista poder julgar questões de facto. Mais tarde, a revista passa a ser um meio de impugnação, que se restringia a questões de direito"[523].

Duplo Grau de Jurisdição: O princípio do duplo grau de jurisdição envolve a revisão de casos por uma segunda instância judicial para garantir a correção de erros de julgamento em busca de decisões justas. Em geral, é necessário que uma causa seja julgada por duas instâncias judiciais distintas, da mesma ordem ou de ordens jurisdicionais diferentes, que é o entendimento de Amâncio Ferreira[524].

Natureza Jurídica do Recurso: A natureza jurídica do recurso é objeto de debate na doutrina jurídica. Existem duas correntes de pensamento: uma que o vê como um remédio no mesmo processo e outra que o considera semelhante a uma

[522] Wladimir Brito (2020: 345)

[523] Wladimir Brito (2020: 340)

[524] Fernando amâncio Ferreira (2005: 77)

ação. Ambas concordam que o recurso é um direito subjetivo público processual, mas diferem em sua natureza. No entanto, ele depende da escolha das partes em utilizá-lo ou renunciá-lo.

Essas informações ajudam a compreender como as partes desempenham um papel ativo na impugnação de decisões judiciais e na solicitação de revisões por meio de recursos.

Recursos

No contexto jurídico, um recurso é um meio específico de contestar decisões judiciais. É um pedido feito pelas partes ou pelo Ministério Público a um tribunal superior para que reavalie uma decisão judicial tomada em um processo, conforme pontua Wladimir Brito ao concordar com alberto dos reis, em "*definir o recurso dizendo que é um meio específico de impugnação de decisões judiciais. Traduz-se sempre num poder concedido por lei às partes e ao Ministério Público de provo-car a actuação de outro Tribunal, normalmente, dentro da mesma ordem jurisdicional*"[525]. A natureza jurídica do recurso é objeto de debate entre juristas, mas geralmente é considerada um direito subjetivo público processual. Existem duas correntes de pensamento sobre sua natureza: uma que o vê como um remédio no mesmo processo em que a decisão foi proferida e outra que o considera semelhante a uma ação. Em ambas as correntes, concorda-se que o recurso é um direito subjetivo, mas sua natureza é interpretada de maneira diferente, conforme já mencionado.

Os recursos são fundamentais para garantir a revisão de decisões judiciais, corrigir erros de julgamento e assegurar a justiça no sistema legal, visto que afirma Wladimir Brito "*Essa tendência levou a que com naturalidade as comunidades humanas aceitassem a impugnação das decisões como uma das formas possíveis de corrigir erros ou injustiças praticados por instâncias decisórias, fossem ou não de natureza jurisdi-cional*"[526]. Eles são regidos por leis e regulamentos específicos, variando de acordo com a jurisdição e o sistema legal em vigor. Os recursos geralmente envolvem um duplo grau de jurisdição, o que significa que a decisão é revisada por um tribunal hierarquicamente superior, em que isso é abordado como um conceito histórico,

É importante destacar que a iniciativa para entrar com um recurso cabe às partes envolvidas no processo. Os tribunais não iniciam recursos de ofício. Portanto, as partes devem solicitar ativamente a revisão da decisão e usar os recursos disponíveis de acordo com a legislação aplicável.

Em resumo, um recurso no contexto jurídico é um meio pelo qual as partes ou o Ministério Público podem contestar decisões judiciais, buscando uma revisão por um tribunal superior. Sua natureza jurídica é objeto de debate, mas, em geral, é

[525] Wladimir Brito (2020: 351)

[526] Wladimir Brito (2020: 336)

considerado um direito subjetivo público processual. Recursos desempenham um papel essencial no sistema legal para assegurar a justiça e a correção de erros judiciais.

Duplo Grau de Jurisdição

O duplo grau de jurisdição é um conceito fundamental no sistema judicial que permite a revisão de casos por uma segunda instância judicial. conforme informa Castro Mendes, "*nisto: a reclamação representa um pedido de revisão do problema sobre que incidiu a decisão judicial, revisão feita pelo mesmo órgão Judicial e sobre a mesma situação em face da qual decidiu; o recurso representa um pedido de revisão da legalidade ou ilegalidade da decisão judicial, feita por um órgão judicial diferente (superior hierarquicamente) ou em face de argumentos espe-ciais feitos valer*"[527]. Ele desempenha um papel crucial na garantia da justiça e na correção de erros judiciais. Em um resumo podemos apresentas seguintes informações que podem ser consideradas principais:

Contestação de Decisões Judiciais: O duplo grau de jurisdição permite que as partes contestem decisões judiciais quando consideram que são injustas ou errôneas. Isso está de acordo com a prática tradicional em sistemas legais e é amplamente aceito, é o que afirma Alberto dos reis, em "*definir o recurso dizendo que é um meio específico de impugnação de decisões judiciais. Traduz-se sempre num poder concedido por lei às partes e ao Ministério Público de provo-car a actuação de outro Tribunal, normalmente, dentro da mesma ordem jurisdicional*"[528].

Meios de Impugnação: No contexto de processos judiciais, existem dois principais meios de impugnação: a reclamação (que inclui os embargos) e o recurso. A principal diferença entre eles é que, na reclamação, o próprio juiz revisa a decisão, enquanto no recurso, a revisão é realizada por um órgão judicial hierarquicamente superior, conforme afirma Castro Mendes[529].

Iniciativa das Partes: As impugnações nos processos judiciais não ocorrem automaticamente. Em vez disso, dependem da iniciativa das partes envolvidas. São as próprias partes que devem solicitar a revisão da decisão, seja por meio de reclamação ou recurso, conforme dito por Wladimir Brito "*Importa finalmente dizer que todas as impugnações dependem da ini-ciativa das partes ou seja nunca são oficiosamente feitas. Têm de ser as par-tes a deduzi-las, pedindo a reapreciação da decisão, estando, portanto, na disponibilidade delas o uso desses meios processuais*"[530]. O que nos leva a finalidade do Recurso: O recurso é um remédio processual utilizado pelas partes ou pelo Ministério Público para solicitar a revisão de uma decisão judicial, com o objetivo de alterá-la. Geralmente, a parte que não concorda com a decisão e se sente prejudicada é quem recorre.

---

[527] Castro Mendes (1980: 3)

[528] Wladimir Brito (2020: 351)

[529] Castro Mendes (1980: 3)

[530] Wladimir Brito (2020: 345)

É sabido conforme apresentado o duplo grau de jurisdição envolve a revisão de casos por uma segunda instância judicial, geralmente hierarquicamente superior à primeira instância. Isso é essencial para garantir a correção de erros de julgamento e alcançar decisões justas.

Natureza do Recurso: O recurso não cria um novo processo, mas é uma fase subsequente do mesmo processo tratada por um tribunal superior. Ele permite a reavaliação da decisão original e a possibilidade de modificá-la, anulá-la ou revogá-la, então conclui Wladimir Brito sobre duas linhas de pensamentos sobre a natureza do recurso "ambas portanto, aceitam a ideia de que o recurso é um direito subjectivo, só divergem na natureza desse direito, sendo para uns de natureza substantiva e para outros de natureza processual"[531].

Constituição e Limites: A Constituição indiretamente aborda o princípio do direito de recorrer, permitindo ao legislador ordinário flexibilidade para escolher como regular o direito de recorrer. No entanto, os limites constitucionais, princípios de igualdade e proporcionalidade não podem ser violados. Wladimir Brito informa que "*apesar desse reconhecimento indirecto do princípio, o Tribunal Constitucional tem entendido que o legislador ordinário pode ou não consagrar o princípio, só não lhe sendo admitido pôr em causa o sistema constitucionalmente estabelecido*"[532].

Sucumbência e Modificabilidade da Decisão: O recurso normalmente requer a existência de uma parte que sucumbe (perde) no litígio e a expectativa de que a decisão desfavorável possa ser modificada por outro tribunal. Estes são considerados detalhes secundários do conceito de recurso, onde Wladimir Brito informa que "*os elementos estruturantes do conceito de recurso são o reexame ou a reponderação, mesmidade do processo e da relação jurí-dico-processual, duplo grau de jurisdição. a sucumbência e a modificabilidade da decisão devem ser qualificados como aspectos acessórios do conceito*"[533].

A natureza jurídica do recurso é um tópico debatido na doutrina. Algumas correntes veem o recurso como um remédio no mesmo processo, enquanto outras o comparam a uma ação, compartilhando a natureza jurídica desta. No entanto, a maioria concorda que o recurso é um direito subjetivo público processual.

Em resumo, o duplo grau de jurisdição desempenha um papel fundamental no sistema jurídico, permitindo a revisão de decisões judiciais por instâncias superiores para garantir a justiça e corrigir erros. É um elemento importante da garantia do devido processo legal e do acesso à justiça.

Conclusão

Em conclusão, este artigo abordou os principais aspectos relacionados à

[531] Wladimir Brito (2020: 355)

[532] Wladimir Brito (2020: 349)

[533] Wladimir Brito (2020: 350)

impugnação de decisões judiciais, com foco nos recursos como um meio fundamental nesse processo. Recapitulando os pontos-chave discutidos em cada seção:

Natureza da Impugnação de Decisões Judiciais: As decisões judiciais podem ser contestadas por meio de reclamação ou recurso, sendo um princípio unânime no sistema legal. Isso ocorre quando as partes consideram as decisões injustas ou errôneas.

Reclamação e Recurso: Existem dois principais meios de impugnação em processos jurídicos, a reclamação e o recurso. A diferença fundamental entre eles está na autoridade que revisa a decisão: na reclamação, o próprio juiz revisa a decisão, enquanto no recurso, a revisão é realizada por um órgão judicial superior hierarquicamente.

Iniciativa das Partes: Tanto a reclamação quanto o recurso dependem da iniciativa das partes. As partes envolvidas devem solicitar ativamente a revisão da decisão, o que destaca a importância da participação das partes no processo.

Objetivo do Recurso: O recurso é um meio de revisar uma decisão judicial com o objetivo de alterá-la, geralmente quando as partes se sentem prejudicadas pela decisão original. Isso é essencial para buscar uma decisão mais justa.

Duplo Grau de Jurisdição: O princípio do duplo grau de jurisdição é fundamental para garantir a correção de erros de julgamento. Isso envolve a revisão de casos por uma segunda instância judicial, buscando uma decisão mais justa.

Constituição e o Direito de Recorrer: A Constituição trata indiretamente do direito de recorrer e deixa ao legislador ordinário a flexibilidade de decidir sobre sua consagração. No entanto, o legislador não pode comprometer o sistema constitucional ao restringir excessivamente o direito de recorrer.

Natureza Jurídica do Recurso: A natureza jurídica do recurso é um ponto debatido na doutrina. Algumas correntes veem o recurso como um remédio no mesmo processo, enquanto outras o comparam a uma ação. Independentemente da visão, é considerado um direito subjetivo público processual.

Em última análise, os recursos desempenham um papel crucial no sistema jurídico, permitindo que as partes contestem decisões judiciais que considerem injustas ou errôneas. Eles representam um meio de buscar justiça e corrigir possíveis erros de julgamento, contribuindo para a integridade do sistema judicial. A participação ativa das partes na busca por uma revisão é um elemento essencial desse processo.

Referências

BRITO, WLADIMIR. Teoria Geral do Processo. Disponível em: Grupo Almedina, Grupo Almedina (Portugal), 2020

FERREIRA, FERNANDO AMÂNCIO (2005) Manual dos recursos em Processo Civil, Ed alme-dina, Coimbra.

GONÇALVES, MARCUS VINICIUS RIOS (2008), Novo Curso de Direito Processual Civil, Vol. I, Ed. Saraiva, S. Paulo (2008), Novo Curso de Direito Processual Civil, Vol. II, Ed. Saraiva, S. Paulo.

MENDES, JOÃO DE CASTRO (1980), Direito Processual Civil, Volume I, Ed. associação aca-démica da faculdade de Direito de Lisboa.

OVÍDIO A. BAPTISTA da (2010) Curso de Processo Civil, Vol. 1, 4.a Edição, revista dos Tribunais.

SOUSA, MIGUEL TEIXEIRA de (1997), Estudos sobre o Novo Processo Civil, Ed. Lex, Lisboa.

O Juiz e a Política: Afinal, podemos dizer que é permitida a participação do Juiz?

José Aparecido Evangelista[534]

Resumo

Como se não bastasse a sociedade ter que administrar os comportamentos mais diversos dos políticos que a representam, e isso por demais é suficiente para tirar o sono e tranquilidade de quem vive em uma sociedade que se diz democrática e

[534] Mestrando em Direito Judiciário pela Universidade Europeia- Portugal; Graduado em Direito pela Faculdade Rio Branco em São Paulo; Pós-graduado em Direito e Processo do Trabalho- Pontifícia Universidade Católica do Rio Grande do Sul; Extensão em Direito Empresarial e Compliance pelas Universidades de Siena na Itália e de Valladolid na Espanha; Especialização em Gestão Empresarial e Relações Sindicais pela Fundação Getúlio Vargas, São Paulo; Pós-graduado em Administração Estratégica de Recursos Humanos pela Universidade Nove de Julho, São Paulo; Formado em Administração pela Universidade Nove de Julho, São Paulo; Com experiência nas áreas de Recursos Humanos e Jurídica em empresas multinacionais; Advogado; Especialista em Relações Trabalhistas e Sindicais, Empresarial e Compliance; Perito Judicial Trabalhista e Previdenciário

valoriza o seu Estado de direito, um tema que tem chamado a atenção nos últimos tempos, em diversos países, incluindo Portugal, é a permissão dos juízes assumirem cadeiras em cargos políticos ou em funções com viés e natureza política, e, se o legislador não se posicionar, teremos de forma notória o que podemos chamar de conflitos de interesses, além de ferir alguns princípios legais e éticos de toda uma legislação desenvolvida através de muitos anos, pois, apenas uma proposta, poderá se tornar uma permissão. Com o texto que foi desenvolvido nestas poucas páginas, temos consciência que estamos longe de ser uma solução para a problemática, mas deixamos a proposta de continuidade, pois é certo que não há como distanciarmos os temas de justiça com os de política, e mesmo que o tema venha a ser questionado, em se tratando dos princípios da independência e da imparcialidade, sempre será notório as questões se os juízes devem ou não participar de forma ativa nas arenas políticas.

Palavras chaves: Administração e política; conflitos de interesse; profissão e atividade do juiz; vocação política.

O Juiz e a Política: Afinal, podemos dizer que é permitida a participação do Juiz?

José Aparecido Evangelista

Abstract

As if it weren't enough for society to have to manage the most diverse behaviors of the politicians who represent it, and this is enough to make you lose sleep and peace of mind when trying to live in a society that calls itself democratic and values its rule of law. , and a topic that has attracted attention in recent times, in several countries, including Portugal, is the condition or permission for judges to assume positions in political positions or in functions with a political bias and nature, and if the legislator does not take a position, We will clearly have what we can call conflicts of interest, in addition to violating some legal and ethical principles of legislation developed over many years, and what is just a proposal could become a permission. With the text that has been developed in these few pages, we are aware that we are far from being a solution to the problem, but we leave the proposal for continuity, as it is certain that there is no way to distance the themes of justice from those of politics, and even if If the topic comes to be questioned when it comes to the principles of independence

and impartiality, the questions of whether or not judges should actively participate in political arenas will always be clear.

Keywords: Administration and politics; profession and activity of the judge; interest conflicts

Introdução

Quando tratamos do tema política, é certo que as discussões tomam rumos dos mais diversos, e não seria diferente ao introduzirmos algo do judiciário que esteja relacionado ou queira se relacionar com a esfera política, mesmo que esteja inserido em ordenamentos de estados considerados democráticos e com respeito ao seu Estado de Direito. Neste prisma, podemos dizer que a política e os juízes e sua participação tem sido alvo de inúmeros debates nos mais diversos países, e um deles, Portugal. Ao expormos o tema em relação aos princípios da independência e da imparcialidade, é notório o questionamento se os juízes devem ou não participar ativamente nas arenas políticas.

Em poucas páginas, nosso objetivo é abordar o tema e alguns pontos que entendemos relevantes para uma introdução e breve crítica sobre o juiz e sua participação nas questões políticas no contexto em que está inserido, em nosso caso, Portugal. Desta forma, é importante termos um pano de fundo, mesmo que de forma muito sintética, de momentos históricos em países próximos, o que consta nos dispositivos legais sobre a profissão e atividade do juiz, a visão da aceitação partidária e da associação dos juízes, bem como alguma jurisprudência para tentar elucidar o tema discorrido, e com isso, tentar aproximar o máximo das ações consequentes do resultado dessa problemática.

No desenvolvimento, vamos ter como norte a questão se "*podemos dizer que é permitida a participação do juiz*?" em um Estado com o sistema democrático, e ainda navegar em situações em que a participação de um juiz tenham vistas

competitiva ou prejudicial para a justiça sem ferir a imparcialidade e se há algum dilema ético que pode surgir com a pretensão de envolvimento na política.

Desta forma, a contribuição que deixaremos aqui, é o de oferecer alguns insights como introdução para a continuidade em debates na questão da participação ou não do juiz na política, visto em uma sociedade considerada democrática, pois bem sabemos que é inevitável em algumas circunstâncias a participação judicial na política, mesmo existindo alguns riscos e desafios para a integridade e independência do judiciário.

1 – O juiz e a participação na política, um breve histórico

Antes mesmo de deixarmos a questão sobre o tema deste artigo, se "*podemos dizer que é permitida ou não a participação do juiz na esfera política*, importante discorrermos um pouco do que está registrado na história visto entre o período da idade média e a marcha buscando a independência corporativa e sua luta pela autoadministração, e assim tentar entender se há relação entre o juiz e a política, onde ficou claro que houve interferência no poder político devido às decisões nos tribunais, mesmo em meia a uma época em que os juízes tinha apenas como função interpretar e aplicar a lei. Para nosso desenvolvimento ser mais direto e produtivo, tomaremos como norte, o exemplo da França em sua luta política e esta com resultados em toda a Europa.

Partindo do período na idade média, onde a justiça havia sido fragmentada e que os chefes locais ou monarcas exerciam a função de julgar por meio dos tribunais senhoriais, situação que levava os juízes a depender de tais senhores. O que tempo mais tarde na situação pode ser notada uma modificação e de forma progressiva e quem agora estabelecia a justiça eram os monarcas, sendo então os juízes nomeados por estes e ainda assim dependentes, considerados agora um emprego de forma a lucrar com isso, o que podemos dizer que a justiça "era" do monarca e que aos poucos foi sendo o juiz conseguindo reconhecimento dentro da hierarquia social e política da época, vindo assim influenciar a atividade política no

exercício de controle com certa permissibilidade e controle da realeza se necessário, com poder advindo em momentos que produziam algumas normas e estas eram utilizadas para tal confronto. Para não serem desprestigiados e serem afastados dos negócios políticos, acontece então uma revolta dos juízes contra o monarca.[535]

No período considerado entre o iluminismo e a famosa revolução francesa, especificamente no século XVIII, há uma mudança na posição dos juízes, onde estes iniciam uma luta buscando sua independência relacionada às questões políticas. A partir deste período, os juízes buscam deixar de ser aquele funcionário real e dependentes do monarca, passando assim ter uma estrutura mais separada e podendo se utilizar de seu poder julgador.

Em continuidade ao movimento, os juízes agora se veem obrigados a lutar pela sua independência individual, pois como vimos até então, tal independência não estava inserida em seu estatuto, de forma que ainda eram vistos como meros funcionários da administração do monarca, melhor dizendo, soldados do Direito. Então, nota-se que a partir do iluminismo podemos ver uma ação positiva por parte da considerada e tradicional nobreza e a de toga, a primeira para manter-se no poder e controle, e a segunda para ter o controle sobre os juízes. Ambas tinham que buscar suporte no judiciário a tentativa de oposição ao poder que possuía o monarca e que na época era absoluto. E vemos um melhor resultado por volta do século XVIII em que tem início à profissionalização, onde a função do juiz mesmo de forma progressiva fica agora nas mãos de juízes profissionais, vindo então criar uma certa resistência contra o poder real. Aqui notamos a evolução, onde os juízes deixam de ser aqueles funcionários da realeza como acontecia na idade média, e passam a ter alguma participação na política de maneira a enfrentar o absolutismo da monarquia.

Juntamente à revolução francesa, o movimento originado pelos juízes vem tomando corpo na sua conquista contra o poder da realeza, o que deixou a todos um pouco assustado, pois a luta que estava sendo demonstrada abertamente, não era só com o objetivo de assegurar a independência como também na tentativa de abater o modelo do antigo regime, onde os tribunais eram os palcos da batalha e

[535] BRITO, Wladimir. Os Juízes e a Política: A origem política do Conselho Superior de Magistratura. Almedina. 2023. Pgs 12 a 16.

os juízes cada vez mais ativos em sua luta política. Fica evidente que a visão de um juiz que apenas servia o monarca, estava agora deixando de ser e se tornando mais fortes, isso entre os séculos XVII e XVIII, onde era notória a intervenção dos juízes na política e se utilizavam de todos os meios do judiciário que estavam a sua disposição. [536]

Vemos ainda próximo da revolução francesa, que os tribunais tinham poder participativo no legislativo e executivo, tanto que era conferido aos juízes um certo poder político que os revolucionários não concordavam. Mesmo em meio a algumas situações consideradas arbitrárias que os juízes cometiam ao participarem na luta contra o poder absoluto da época, de certa forma se tornaram relevantes e figuravam no cenário político como atores.

Vemos até aqui uma importante participação dos juízes deixando impressa a vitória não somente ao que se refere no direito, mas a formação de um corpo judicial e político na luta contra o considerado regime e o monarca. Os juízes nesse momento não eram considerados pelos revolucionários como de confiança, pois sendo perigosos precisavam ser neutralizados e terem a espada tirada de suas mãos, ou seja, a justiça. Isso por conta do medo e receito dos juízes e a magistratura se virar contra o processo da revolução.

O mais importante agora era saber então se essa imagem que tinham os revolucionários sobre os juízes havia mudado após a revolução, fazendo com que a desconfiança deixasse de ser, pois com a queda do absolutismo era esperado também que o modelo da magistratura de até então não seria mais necessário. Montesquieu tinha plena consciência da capacidade dos juízes em se pensando na atuação em corpo de magistrado, isso pela força relevante de que podiam para se combater o absolutismo, visto a tal força que a lei tinha e gerava muitos abusos e também injustiças. Algumas situações com a revolução levaram a buscar o controle do judiciário, o que não foi de bons olhos para os juízes que não aceitavam ser supervisionados senão por sua classe, e esta garantir sua independência. Com isso vem o legislativo na tentativa de controlar o poder dos juízes e estes submissos à lei, e então considerados como sendo a boca da lei apenas. Mesmo com o fim da fase absolutista, a luta não finda com o intuito de afirmar a independência dos juízes e

[536] BRITO, Wladimir. Os Juízes e a Política: A origem política do Conselho Superior de Magistratura. Almedina. 2023. Pgs 17 a 21.

fazer libertar-se do controle das forças conservadoras, e não apenas neutralizar os juízes fazendo apenas como se fosse a boca da lei. [537]

Com vistas a criar um modelo em que tivessem um juiz neutro e apolítico, os revolucionários seguiram na tentativa através do poder legislativo, visto que só ele teria condições de interferência nas questões da atividade judicial, de modo a fazer que o juiz apenas viesse aplicar a lei e esta literalmente e em nada de interpretação, o que ficou claro que o juiz agora dependia somente da lei, e agora com mais controle com algumas soluções como por exemplo eleger o juiz por apenas um limite de tempo e um tribunal para a punição dos juízes. Isso nos leva a entender sendo uma certa responsabilidade do juiz perante a nação, e que os juízes não devem jamais interferir nas atividades do poder legislativo, bem como na administração, visto como sendo uma máquina de subsunções, um modelo ideal de atuação para o juiz dessa época, mesmo com tentativas de manifestação pelas conquistas de outrora.

Até aqui temos que fazer o reconhecimento do que chamamos de inamovibilidade e com uma conquista no fim do antigo regime, ou melhor dizendo, sua independência individual. Nesse momento, a função do juiz tinha que ter prestação de contas ao legislativo. Os juízes eram proibidos de interpretar a lei, vindo então como obrigação a dependência desse legislativo no que se referia à interpretação da lei, o que poderia culminar na punição do juiz por violação ao que lhe era determinado em suas atividades.

Com tudo isso e vindo a revolução francesa, então surge o interesse na construção do estatuto do juiz, onde constavam alguns pontos de garantia como a inamovibilidade, a independência individual, responsabilidade dos juízes junto ao legislativo, a proibição de interpretar as leis e a punição vinda por um tribunal. Com esse modelo, fica evidente o controle político estar com o legislativo, impedindo o juiz de uma atuação política. Tal situação não teve melhora, pois com o passar dos tempos, o poder soberano passa a submissão do juiz para a soberania da lei, e esta era dominada pela burguesia, tornando então o juiz em uma condição de funcionário, o que futuramente esses juízes se submetiam ao executivo que fazia toda

[537] BRITO, Wladimir. Os Juízes e a Política: A origem política do Conselho Superior de Magistratura. Almedina. 2023. Pgs 22 a 29.

a sua gestão. A verdade é que, desde a pretensão da revolução francesa, tanto os avanços como recuos relacionados ao poder político e posicionamento dos juízes, tinham como centro a sua inamovibilidade e com esta sua independência individual, bem como a liberdade de fazerem a interpretação da lei, isso até o final do século XIX.[538]

Com todo o exposto, mesmo que de forma sumária, ainda podemos referenciar algumas escolas ou doutrinas, como melhor entender, que tiveram posicionamento contra tal legalismo. Podemos iniciar com a Escola Histórica alemã, que tinha sua discordância fundamentada em não aceitar o monopólio da lei dizendo que os códigos dificultavam a evolução do direito da forma natural. Já vemos que na jurisprudência dos conceitos defendida por Puchta e Rodolf, dizendo que a utilização de conceitos oferece melhor compreensão do direito, isso através de elaboração de critérios. A escola do direito livre vem com a defesa de que a aplicação da norma pode ser decisiva ao se utilizar a personalidade do juiz, onde podemos dizer que isso é uma atividade exclusivamente pessoal e individual da pessoa de cada juiz. Podemos citar ainda a jurisprudência dos interesses, onde em certos pontos diverge das anteriores, mas com a diferença de que ao juiz é conferida uma justificação doutrinal na reivindicação do seu direito, onde o juiz pode até mesmo ser considerado um dos criadores de direito, mesmo que tenha alguma subordinação ao legislativo, onde a visão do juiz agora era de que aceitava sua condição de serventuário da lei.

Diante do até aqui exposto, fica a impressão de que a existência do que podemos chamar de juiz neutro e apolítico não existe, mas na realidade o juiz agora é uma fonte do direito, isso devido ao longo percurso na luta pela sua independência que, foram estes objetivos que levaram não deixar o controle de toda magistratura na mão dos demais poderes. Visto o até então, não podemos deixar de fazer algumas referências históricas em que juízes estavam envolvidos em atividades políticas, principalmente nos temas referentes a constitucionalidade, dentre os quais podemos citar o Juiz Coke sobre o caso Bonham na Inglaterra em 1610, como sendo o princípio de tudo, o Jurie Constitucionnaire com a influência de Abade de Sièyes na França em 1799, o caso Marbury vs Madison em 1803 do Juiz Marshall nos Estados

[538] BRITO, Wladimir. Os Juízes e a Política: A origem política do Conselho Superior de Magistratura. Almedina. 2023. Pgs 30 a 34, 38 a 42.

Unidos, e mais tarde em 1835 o tribunal constitucional da Áustria e Suíça motivados pela teoria de Sièyes. Tais casos aqui referenciados, foram os que nos deixaram a memória na evolução de uma luta política dos juízes, mas agora na conquista de uma independência mais coletiva.[539]

Dentre esses, podemos dizer que o maior destaque se deu pelos juízes franceses que sempre se movimentaram para fazer prevalecer seus direitos com relação a inamovibilidade, interpretação das leis e o controle das leis com base na constituição e não deixar o controle dos tribunais com os demais poderes. Isso deixa claro e notório a presença e participação dos juízes franceses com envolvimento na política e também pela política.

Com o que expomos, passamos a partir de agora, a entrar nas questões em que a legislação de Portugal tem como previsão sobre a vida profissional e as atribuições aos juízes atualmente, e dessa legislação tomaremos como base o código de ética dos advogados de Portugal, o compromisso ético da associação sindical dos juízes portugueses, o estatuto dos magistrados de Portugal, requisitos da comissão nacional de eleições e a constituição da república.

2 – Base legal sobre a atividade do juiz em Portugal

Apresentado um pouco do cenário sobre o tema, e como deixou o professor Wladimir Brito, entendemos que o juiz tem condições de influenciar as questões políticas e atuar nessa seara. Então vejamos o que vem expresso nas normas e temas correlatos para aproximarmos um pouco mais da problemática se "*podemos dizer que é permitida a participação do Juiz nas questões políticas*".

2.1 – Constituição da República de Portugal - Decreto de 10 de abril de 1976

Vejamos de início o que encontramos na CRP, especificamente no Artigo 216º, número 3, onde é evidente a incompatibilidade de forma expressa e que "*Os juízes em exercício não podem desempenhar qualquer outra função pública ou privada, salvo as funções docentes ou de investigação científica de natureza jurídica, não*

[539] BRITO, Wladimir. Os Juízes e a Política: A origem política do Conselho Superior de Magistratura. Almedina. 2023. Pgs 45 a 52, 60 a 69, 83.

remuneradas, nos termos da lei.". Em uma simples leitura, nota-se que tal proibição é no sentido geral, ou seja, veda a atuação do juiz a desempenhar as atividades estranhas ao que lhe diz respeito a função como julgador, vindo colocar em risco sua independência através de algumas situações financeiras e profissionais. Importante dizer ainda que tal prática ou até mesmo com cargos simultâneos, podem gerar alguns inconvenientes para o serviço público onde está inserido tal juiz.[540]

2.2 – Estatuto da Ordem dos Advogados de Portugal - Lei 145/2015 de 09/09

Antes de seguirmos, entendo como importante comentar alguns artigos do estatuto dos advogados, visto que é uma base de onde se origina os primeiros passos na vida antes mesmo de se tornar um juiz e a formação de sua estrutura deontológica, pois a deontologia é a marca da advocacia, onde fica evidente que o advogado se mostra apto e capaz de exercer sua função e desta vindo a confiança individual ou coletiva, e nestes associados o direito e a moral. Podemos começar falando do artigo 88º sobre a integridade, onde destacamos a importância do advogado para uma boa administração da justiça, e deste comportamento se originam outros mais como honestidade, probidade, retidão, lealdade, cortesia e sinceridade, que são obrigadas a tais profissionais, e tudo sendo considerado de forma espontânea para que seja reconhecido como indispensável para a sociedade. É sabido que uma relação pautada na confiança só existe se os comportamentos mencionados anteriormente forem inquestionáveis. Já o artigo 89º fala sobre a independência, onde vemos como um dos principais atributos para o exercício da advocacia, senão o principal, onde se exige a vivência livre de toda e qualquer pressão, principalmente as que possam vir do seu próprio interesse ou das influências externas. E por fim, o artigo 90º sobre os deveres com a comunidade, onde podemos destacar que o primeiro compromisso do advogado é com a justiça e seus serviços, e como um princípio que vem dignificar e responsabilizar sua profissão, onde sua obrigação é lutar contra leis injustas e ou iníqua. [541]

[540] BRANCO, C. C e ALMEIDA, J. E. Estatuto dos Magistrados Judiciais Anotado e Comentado. Almedina. 2023. Pags 184/185.

[541] MAGALHÃES, F. S. Estatuto da Ordem dos Advogados. Anotado e Comentado. Almedina. 2023. Pags 122/126.

2.3 – Estatuto dos Magistrados Judiciais de Portugal - Lei 21/85 de 30/07

Se tivéssemos que apenas nos pautar no que deixa expresso a Constituição e o Estatuto da Ordem dos Advogados de Portugal, por certo já teríamos matéria suficiente para um posicionamento, isso para se "*podemos dizer que é permitida a participação do Juiz nas questões políticas*". Mas por se tratar de um tema um pouco delicado e não causar maiores traumas, vamos adentrar em alguns artigos do Estatuto dos Magistrados, visto que para o exercício da magistratura bem sabemos que é preciso uma conduta compatível e esta com preceitos positivados para nortear os passos dos juízes, e aqui destacarei a incompatibilidade e a proibição de atividades políticas, dos artigos 8º-A, número 1[542] e 6º-A[543] respectivamente.

Em conjunto com o artigo 216º da Constituição, o artigo 8º-A número do Estatuto dos Magistrado mostra-se não permitir que o magistrado ativo e em fase de jubilação tenha atuação em funções estranhas às que atualmente tem no judiciário, a de julgar, visto como já mencionado, vindo colocar em risco sua independência através de algumas situações financeiras e profissionais, onde pode se destacar a inelegibilidade relativa, posto que tal pessoa poderá ocupar cargos eletivos e de nomeação, e na inelegibilidade absoluta em que se preenche os requisitos estabelecidos por lei na admissão deste individuo para um determinado cargo público ou outro que não seja. Sendo assim, a incompatibilidade mostra ser impossível a coexistência de duas qualidades que se excluem. Sendo possível somente com a renúncia do cargo atual de forma expressa ou se existir determinação legal. Em resumo, o juiz jamais deve se colocar em posições onde sua independência e imparcialidade venham ser questionadas.[544] Já o que vem expresso no artigo 6º, notamos que o legislador foi taxativo na questão da proibição

[542] Artigo 8.º-A – Incompatibilidades - 1 - Os magistrados judiciais em efetividade de funções ou em situação de jubilação não podem desempenhar qualquer outra função pública ou privada de natureza profissional.

[543] Artigo 6.º-A - Proibição de atividade política - 1 - É vedada aos magistrados judiciais a prática de atividades político-partidárias de caráter público. 2 - Os magistrados judiciais não podem ocupar cargos políticos, com exceção dos cargos de Presidente da República, de membro do Governo, de membro do Conselho de Estado ou de Representante da República para as regiões autónomas.

[544] BRANCO, C. C e ALMEIDA, J. E. Estatuto dos Magistrados Judiciais Anotado e Comentado. Almedina. 2023. Pags 184/185.

dos magistrados em atividades políticas, onde tal preceito se estende também aos que se encontram jubilados e quando do seu envolvimento, mesmo nas consideradas não públicas, é de se rejeitar e sua participação deveria estar consagrada em legislação. E como se não bastasse, no mesmo dispositivo em seu artigo 83º-G, alíneas C e I[545], ficou expresso que o envolvimento em atividades de caráter político-partidárias, é considerada infração muito grave. Vejamos que tudo está expresso no estatuto, e vem na mesma linha com os artigos 27º e 28º da Lei Orgânica do Tribunal Constitucional.[546]

2.4 – Associação Sindical dos Juízes Portugueses - Lisboa 2009

"Se o cidadão tiver dúvidas quanto ao Sistema Judicial, que tenha sempre confiança nas qualidades dos juízes portugueses para realizarem a Justiça, "dando a cada um o que é seu".

António Martins

Presidente da Associação Sindical dos Juízes Portugueses

Para a associação e dentro do compromisso ético dos juízes portugueses, a ética judicial tem como base, alguns atributos onde deve o juiz centrar-se, dentre eles a independência, imparcialidade, integridade, humanismo, diligência e reserva, e dentre estes vamos apenas pontuar dois deles não com mais importantes e sim como

[545] Artigo 83.º-G - Infrações muito graves - Constituem infrações muito graves os atos praticados com dolo ou negligência grosseira que, pela reiteração ou gravidade da violação dos deveres e incompatibilidades previstos no presente Estatuto, se revelem desprestigiantes para a administração da justiça e para o exercício da judicatura, nomeadamente: c) O exercício de qualquer atividade incompatível com a função, ainda que o magistrado judicial se encontre na situação de jubilação; i) A prática de atividade político-partidária de caráter público;

[546] Lei Orgânica do Tribunal Constitucional - Lei n.º 28/82, de 15 de novembro. Artigo 27.º - Incompatibilidades. 1 - É incompatível com o desempenho do cargo de juiz do Tribunal Constitucional o exercício de funções em órgãos de soberania, das Regiões Autónomas ou do poder local, bem como o exercício de qualquer outro cargo ou função de natureza pública ou privada. 2 - Excetua-se do disposto na parte final do número anterior o exercício não remunerado de funções docentes ou de investigação científica de natureza jurídica; e Artigo 28.º. Proibição de atividades políticas. 1 - Os juízes do Tribunal Constitucional não podem exercer quaisquer funções em órgãos de partidos, de associações políticas ou de fundações com eles conexas, nem desenvolver atividades político-partidárias de caráter público. 2 - Durante o período de desempenho do cargo fica suspenso o estatuto decorrente da filiação em partidos ou associações políticas.

relevantes para seguirmos com nossa problemática, a saber, a independência e imparcialidade.

Para a associação dos juízes, a independência tem que estar fortemente destacada para que seja garantida o estado democrático e uma boa gestão da administração, onde a consequência será de uma justiça imparcial representando os direitos dos cidadãos, vindo assim respeitar sua atuação tanto dentro como fora de sua função, garantindo a imparcialidade e a confiança pública da justiça, onde deve rejeitar em participar de atividades políticas ou mesmo administrativas que venham implicar em subordinar-se a outros órgãos estranhos ao seu de origem. Já a imparcialidade é considerada um dos atributos fundamentais para a atuação do juiz na justiça, onde vem a garantir um direito justo a todos os cidadãos e também equitativo, afastando qualquer dúvida sobre sua atuação referente a este atributo, afastando-se de qualquer atividade que gerem atritos ou condicionem sua confiança junto aos cidadãos e sendo considerado uma pessoa razoável e de boa fé. Desde que o juiz não deixe comprometer sua imparcialidade e atividade jurisdicional, é livre para participar de atividades cívicas. O juiz não deve jamais se associar a coletividades e também não participar de debates públicos, pois isso pode e muito perturbar sua confiança e imagem, bem como de se filiar a algum partido político.[547]

2.5 – CNE - Comissão Nacional de Eleições – 2023

E por fim, podemos deixar registado que, até mesmo a proibição é bem clara junto ao órgão da comissão nacional de eleições, onde vem apresentar algumas pessoas e cidadãos não elegíveis, e dentre estas estão os magistrados judiciais ou do ministério público em efetividade de serviço e os juízes em exercício de funções.[548]

[547] COMPROMISSO ÉTICO DOS JUÍZES PORTUGUESES: PRINCÍPIOS PARA A QUALIDADE E RESPONSABILIDADE – LISBOA. Associação Sindical dos Juízes Portugueses. 8º Congresso dos Juízes portugueses. 2008

[548] https://www.cne.pt/faq2/96/3

3 – Jurisprudência

3.1 - Caso MAESTRI c. ITÁLIA, TEDH acórdão de 17/02/2004. Grande Chambre ou Tribunal Pleno

O juiz Maestri foi sancionado por pertencer à maçonaria, o que teria violado o artigo 11º da CEDH, no sentido de haver total incompatibilidade entre os compromissos do juiz e do maçon, o qual rejeitaria a justiça do Estado no lugar da justiça da maçonaria. Nas palavras de Maestri, tal sanção não é cabível, pois vai contra o seu direito de liberdade de associação. [549]

3.2 - Caso ALBAYRAK c. TURQUIA, TEDH acórdão de 31/01/208, 3ª Seção.

Considerado por um comportamento em conflito, isto por se considerar ter simpatia pelo Partido Trabalhista do Curdistão, que é uma organização armada ilegal, manifestando opinião de que se fosse tirado da magistratura se juntaria sem problemas a tal partido em uma organização na Alemanha. Tal conduta tinha ferido a imagem e honra dos juízes, também a dignidade do poder judiciário e diretamente o respeito pela função exercida atualmente.[550]

4 – Discussões sobre juízes que vão para a política não devem voltar aos tribunais

O tema vem sendo bastante discutido dentro e fora das instituições, e passo a mostrar qual tem sido a posição do Supremo Tribunal de Justiça, Conselho Superior de Magistratura e Associação Sindical dos Juízes de Portugal, o que poderemos ver nos conteúdos deixados neste trabalho conforme os anexos.

4.1 - Supremo Tribunal de Justiça

Para o presidente do STJ, mesmo que a saída dos magistrados não tenha reposição rápida, sua proposta mesmo não sendo vista com bons olhos, pela questão da transparência, é tempo de rever as condições do regime das comissões de serviços

[549] SUMÁRIOS DE JURISPRUDÊNCIA – 2004. Ministério da Justiça – Agente de Portugal junto ao TEDH

[550] BRANCO, C. C e ALMEIDA, J. E. Estatuto dos Magistrados Judiciais Anotado e Comentado. Almedina. 2023. Pags 100/101.

com relação a cargos políticos ou funções com viés e natureza política, não que estas não sejam dignas, deixou claro que, ao decidir pelo caminho da magistratura, que seja definitivo, e se a vocação política se destacar durante este período, o mesmo não deverá ter permissão para retornar à carreira nos tribunais.[551]

4.2 – Conselho Superior da Magistratura

A proposta do CSM é de que, os juízes que optarem pela ocupação de cargo político, terão o cumprimento obrigatório do período de nojo de três anos, podendo retornar como assessores e com perda da antiguidade. Tal regra se aplicará para os juízes que vierem ocupar cargos políticos ou aqueles públicos de alta escala. Quem era juiz ativo na primeira instância assessorará um tribunal de relação e se desembargador, será suporte aos colegas do Supremo.[552]

4.3 – Associação Sindical dos Juízes de Portugal

Em suas considerações, o presidente da associação diz que atualmente a lei tem condições suficientes de fechar o que ele chama de "portas giratórias" que existe entre a atuação política e da justiça, e que a proposta vinda do CSM se torna um passo desnecessário distanciando a melhoria que pretendem, pois com os dispositivos atuais podem fazer a recusa para que os juízes tenham participação em comissões que são inconvenientes seja por qual razão for.[553]

5 – Considerações finais

Usando das palavras de Luís Eloy Azevedo, onde escreveu para a revista Julgar Número 4 de 2008.

> "Mais do que uma profissão, a magistratura judicial é um sacerdócio. O Magistrado tem confiado à sua guarda alguns dos mais altos valores da convivência social, consumindo

551 https://www.dn.pt/politica/magistrados-que-vao-para-a-politica-nao-devem-voltar-aos-tribunais-14784346.html em 19/05/2023

552 https://www.publico.pt/2023/03/08/sociedade/noticia/juizes-ocuparem-cargos-politicos-poderao-cumprir-periodo-nojo-tres-anos-2041671 de 16/05/2023

553 https://observador.pt/2023/03/16/lei-atual-ja-permite-fechar-as-portas-giratorias-entre-politica-e-justica-diz-asjp/ em 19/05/2023

> grande parte da vida a punir os outros, em nome do Direito, pelas violações dos princípios ético-jurídicos que a sociedade pretende incarnar. Para tarefa de tamanha responsabilidade encontrar ambiente adequado, necessita o magistrado de conquistar, não apenas no complexo exercício da função pública, mas também no domínio da vida privada, a autoridade moral e o prestígio social indispensáveis ao exercício da actividade jurisdicional. O magistrado tem de esforçar-se por ser, numa palavra, o espelho das virtudes que, por delegação embora do Direito, a todo o momento exige dos outros."

Ao considerarmos o texto acima, fica evidente que ao magistrado cabe seguir suas funções primordiais embasadas em princípios éticos, pois este lhe fará ser confiante em meio a sociedade com sua conduta e autoridade moral, e por certo refletirá seu compromisso com uma prestação de serviços públicos firmados na excelência ao distribuir a Justiça, o que vem a trazer fortalecimento e legitimar a atual do Poder Judiciário, e dessa forma os princípios éticos serão cultivados para atuar também na função de educar a cidadania. Digo isso, pois é evidente que ao magistrado cabe evitar todo tipo de procedimento que seja incompatível com a dignidade, honra e decoro das funções que lhes são pertinentes e assim ter em seu histórico a prática e conduta de uma vida pública ou particular irrepreensível. Podemos ver com isso que, há uma necessidade do juiz se comprometer pessoalmente os princípios democráticos, valorizando de forma devida à equidade e a justiça, isso além da sua responsabilidade jurídica e social, onde a eficácia desses controles será notada na responsabilidade moral do juiz junto sua própria consciência, assim não sendo necessário nenhum procedimento externo para sua manifestação, tem que ser natural. Dito isto, devemos entender que a justiça, ou alguma atividade desenvolvida em seu nome, seja uma atividade apolítica, e então dizemos que não é suficiente ao juiz ter independência, imparcialidade e competência, mas que tudo isso seja refletido na sua atuação junto à comunidade.

Partindo deste cenário e com tudo que apresentamos, passo a descrever o que, mesmo sendo o juiz uma pessoa super capacitada tecnicamente, moralmente aceita pela sociedade, a problemática se "*podemos dizer que é permitida a participação do Juiz na política*" sempre irá existir e o questionamento sempre será feito se tal pessoa consegue mesmo separar as áreas de modo a não se envolver

mais na política deixando ser levado como muitos por decisões e atuações parciais, pois é assim que atuam quando vemos nas apresentações dos seus projetos políticos.

Então seguimos, como foi apresentado em um breve cenário histórico, os juízes tiveram sempre a iniciativa para se fazer valer sua atuação nos contextos políticos, isso para não deixarem se dominar por outros poderes que não o da sua atuação, ou seja, o judiciário, o que faria ser dele apenas um figurante sem poder de atuação e gestão de tudo que se relaciona aos termos da lei.

Visto de um ponto de vista democrático e independente, segundo o professor Wladimir de Brito, em sua recente obra *Os Juízes e a Política, a origem política do Conselho Superior da Magistratura*, deixa claro que os juízes têm sim condições para atuar na esfera política, por questão de sua independência coletiva através de uma instituição própria para sua administração, ainda terá que aguardar uma oportunidade no sentido de outorga e este com mecanismos de controlo de sua conduta disciplinar. Para ele, é certa que toda participação ou envolvimento de juízes na política, pode ser considerada um mito.

Se um mito ou não, o entendimento que podemos extrair a partir dos dispositivos legais, órgãos e instituições que tem relação com as atividades dos juízes, é bem cristalino que a proibição existe e tem que ser respeitada, e partindo do que a própria constituição de Portugal deixa expresso, o estatuto da Ordem dos Advogados, o estatuto dos Magistrados e a Associação Sindical, os juízes em exercício não podem desempenhar qualquer outra função pública ou privada, pois tal prática coloca em descredito todo o Poder Judiciário, levando em consideração o discurso do presidente da Associação Sindical que, o vai e vem de juízes que ele chama de "porta giratória", de certa forma pode trazer sim "contaminações" para todo aquele que um dia exercer atividade estranha ao da magistratura, isso porque, hoje ele atua na justiça contra alguém que seja de algum partido ou instituição política e amanhã está sentado à mesa com o próprio discutindo temas cotidianos, o que não faz o menor sentido para quem está de fora, no caso a sociedade que dependia de julgamentos e sentenças deste juiz agora participante de atividades fora do judiciário.

E por fim, segundo a base legal disponível atualmente não seja claro para frear tais comportamentos dos juízes, por certo fez o Conselho Superior da Magistratura ao entrar com a proposta para todos aqueles juízes que então decidir em ocupar cargos políticos, que seja submisso ao literal cumprimento do período de nojo de três anos, e sendo que um dia possa retornar, que seja como um assessor e perdendo o benefício da antiguidade, não importando em qual escala ou instância tinha como atuação. Tal proposta não tem condições de resolver ou responder a problemática, se "*podemos dizer que é permitida a participação do Juiz na política*", mas por certo será um grande filtro e com isso não macular o sistema do judiciário admitindo comportamentos que são duvidosos aos olhos de toda a sociedade que depende e espera uma justiça clara dos que atuam na pessoa de juiz.

Feliz o presidente do Supremo Tribunal de Justiça em suas palavras, ao dizer que a aspiração para cargos fora da magistratura não sejam dignas, mas que ao decidir pelo caminho da magistratura, que este seja definitivo, e caso a vocação política venha se destacar durante este período, o mesmo não deverá ter permissão para retornar à carreira nos tribunais.

Referências Bibliográficas

BRANCO, C. C e ALMEIDA, J. E. Estatuto dos Magistrados Judiciais Anotado e Comentado. Almedina. 2023

BRITO, Wladimir. Os Juízes e a Política: A origem política do Conselho Superior de Magistratura. Almedina. 2023

MAGALHÃES, F. S. Estatuto da Ordem dos Advogados. Anotado e Comentado. Almedina. 2023

ASSOCIAÇÃO SINDICAL DOS JUÍZES DE PORTUGAL

https://www.asjp.pt/2010/04/28/compromisso-etico-dos-juizes-portugueses/

COMISSÃO NACIONAL DE ELEIÇÕES DE PORTUGAL

https://www.cne.pt/faq2/96/3

CONSTITUIÇÃO DA REPÚBLICA PORTGUESA
https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

ESTATUTO DA ORDEM DO ADVOGADOS DE PORTUGAL

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2440&tabela=leis&so_miolo=

ESTATUTO DOS MAGISTRADOS DO JUDICIÁRIO

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=5&tabela=leis#:~:text=Aos%20magistrados%20judiciais%20devem%20ser,funcionamento%20da%20administra%C3%A7%C3%A3o%20da%20justi%C3%A7a.

Anexos

Anexo I

"Magistrados que vão para a política não devem voltar aos tribunais"

"Pouco diálogo, nenhuma concertação e muito distanciamento", disse o presidente do STJ. Na abertura do ano judicial defendeu que as comissões de serviço dos magistrados devem ser repensadas. "Se a vocação política despontar no percurso de magistrado, a opção por esse novo caminho não deverá permitir o regresso à judicatura", declarou

Política ou magistratura. Quem vai não deve voltar

A concluir a sua intervenção, Henrique Araújo assinalou que "uma das grandes preocupações dos tribunais comuns é o **envelhecimento das magistraturas**".

"Como tenho apontado em diversas ocasiões, o acesso às Relações e ao Supremo Tribunal faz-se muito tardiamente. A promoção ao Supremo verifica-se, em regra, quando já se está muito próximo da idade que permite a jubilação", assevera.

Paralelamente, **"a saída de magistrados do sistema não tem sido compensada anualmente com a entrada de novos magistrados, uma vez que o número daqueles excede o destes"**.

Por isso "é preciso intervir já, nomeadamente através da alteração da lei de acesso ao Centro de Estudos Judiciários e do reforço da sua capacidade formativa. Esta é, provavelmente, a questão mais candente, mais prioritária".

E deixa uma proposta que pode desagradar a alguns magistrados: "É necessário, **em nome do princípio da transparência, repensar o regime das comissões de serviço** de magistrados judiciais para cargos políticos ou para o exercício de funções relevantes de natureza política, tão nobres e dignas como as funções judiciais. **Quando se escolhe a magistratura como profissão, essa escolha deve ter-se por definitiva. Se a**

vocação política despontar no percurso de magistrado, a opção por esse novo caminho não deverá permitir o regresso à judicatura".
https://www.dn.pt/politica/magistrados-que-vao-para-a-politica-nao-devem-voltar-aos-tribunais-14784346.html acessado em 19/05/2023

Anexo II

Juízes que ocuparem cargos políticos poderão ter que cumprir período de nojo de três anos

Proposta aprovada pelo Conselho Superior da Magistratura para vingar terá que ter aval do Parlamento. Juízes podem regressar aos tribunais, mas perdem antiguidade e ficam obrigados a ser assessores.

Mariana Oliveira

8 de março de 2023, 21:12

Os juízes que saírem para ocupar cargos políticos poderão, no fim, regressar à magistratura, mas serão obrigados a cumprir um período de nojo de três anos, em que deixarão de tomar decisões judiciais e passarão a assessorar outros colegas. É pelo menos isso que prevê a proposta de alteração ao Estatuto dos Magistrados Judiciais aprovada esta quarta-feira no plenário do Conselho Superior da Magistratura (CSM), que teve o apoio da maioria dos seus elementos.

Oficialmente, o CSM confirmou que a proposta de alteração foi aprovada e que será encaminhada para o Ministério da Justiça, mas não divulgou o seu conteúdo. Caberá ao Governo decidir se avança com uma proposta de lei que, para vingar, terá que ter o aval da maioria dos deputados no Parlamento, já que esta é uma matéria reservada da Assembleia da República.

Segundo o PÚBLICO apurou, a sugestão para se avançar com uma proposta neste campo foi feita pelo presidente do Supremo Tribunal de Justiça, Henrique Araújo, que preside por inerência ao CSM, e tem defendido publicamente que os magistrados que optem pela política não devem poder regressar aos tribunais. Não foi, contudo, essa a solução que vingou, após ter sido criado um grupo de trabalho no seio do CSM para analisar esta questão.

Actualmente, quando um juiz quer ir ocupar um cargo político (com poucas excepções como lugares ministeriais, que não necessitam de aval) tem que pedir autorização ao CSM, que avalia se não existe um "prejuízo sério para o serviço", se

em causa está uma função que representa "um interesse público relevante" e se a saída não prejudica "a imagem de independência ou o prestígio da magistratura judicial". Se for dada autorização, o juiz sai (pode optar muitas vezes pelo salário de origem) e o tempo que esteve fora conta como se tivesse estado na magistratura.

O CSM propõe que para saírem para cargos políticos os juízes deixem de ficar sujeitos a uma autorização sua, mas sejam obrigados a pedir uma licença sem vencimento. Quer ainda que o tempo que estiverem fora não seja contado para efeitos de antiguidade, o que vai prejudicar o magistrado na progressão da carreira. A ideia é aplicar este regime a quem sair tanto para cargos políticos, como para outros cargos públicos.

Será assessor quando regressar à magistratura

De fora ficam apenas as comissões de serviço de natureza judicial, que incluem os juízes que vão dar aulas para a escola dos magistrados (Centro de Estudos Judiciários), os que vão inspeccionar os colegas, os que estão no próprio CSM ou os que ocupam cargos judiciais no estrangeiro.

O período de nojo dos três anos só se aplica a quem ocupou cargos políticos ou altos cargos públicos. Quando regressa, se o juiz estava na primeira instância será obrigado a ser assessor num tribunal da Relação e, se era desembargador, será colocado a apoiar os colegas do Supremo. Se estiver colocado neste tribunal de topo deverá ficar na secção social (que decide questões laborais). A proposta do CSM quer ainda baixar o tempo máximo que um juiz pode estar de licença fora da magistratura de 15 para 12 anos.

Na abertura do ano judicial que passou, o presidente do Supremo defendeu que a saída da magistratura para a política deve ser um caminho sem regresso: "Se a vocação política despontar no percurso de magistrado, a opção por esse novo caminho não deverá permitir o regresso à judicatura. Quando se escolhe a magistratura como profissão, essa escolha deve ter-se por definitiva."

Na sua intervenção, Henrique Araújo mostrou-se ainda muito preocupado com a falta de magistrados que já se nota, mas que poderá agravar-se de forma a comprometer o funcionamento dos tribunais.

Uns dias mais tarde defendeu, no Porto, o fim das portas giratórias entre a magistratura e a política. "O fim das portas giratórias trará mais transparência à Justiça. Contra ventos cada vez mais fortes e marés cada vez mais revoltas,

empenhar-me-ei na luta por esse objectivo, o que implicará, pelo menos, a indispensável alteração do Estatuto dos Magistrados Judiciais", fez questão de sublinhar em Abril do ano passado.
https://www.publico.pt/2023/03/08/sociedade/noticia/juizes-ocuparem-cargos-politicos-poderao-cumprir-periodo-nojo-tres-anos-2041671 acessado em 16/05/2023

Anexo III

Lei atual já permite fechar as "portas giratórias" entre política e justiça, diz ASJP

Associação Sindical de Juízes admite que a lei é suficiente para fechar "portas giratórias" entre justiça e política. Representante da ASJP admite estar "totalmente de acordo com o princípio".

O presidente da associação de juízes entende que a atual lei é suficiente para fechar as 'portas giratórias' entre justiça e política e que há uma relação de "duplo interesse" que leva a aplicar a lei "de forma insuficiente".

Em declarações à Lusa, Manuel Soares, presidente da Associação Sindical dos Juízes Portugueses (ASJP) disse que a recente proposta do conselho superior para limitar a circulação de juízes entre carreiras, com passagens pela política e regressos à justiça, já tinha sido avançada pela própria associação em momentos anteriores, estando por isso "totalmente de acordo com o princípio" subjacente.

Mas afirmou também que alterar o Estatuto dos Magistrados Judiciais (EMJ), como pretende o CSM, segundo a proposta tornada pública na semana passada, pode ser um passo desnecessário.

> *O CSM não precisa de lei para nada para fazer melhor do que faz, porque o estatuto atual já dá ao CSM o poder para recusar a ida de juízes para comissões de serviço que considerem inconvenientes por qualquer razão", explicou.*

E, portanto, "se o CSM já tem este poder e que a meu ver exerce de forma insuficiente e com uma malha de exigência muito larga, a minha única observação é esta: com certeza podemos melhorar a lei, mas antes disso porque não exercem os poderes que têm e porque não são muito mais escrupulosos nas autorizações?", questionou.

Manuel Soares disse também ter "as maiores dúvidas" de que o parlamento aprove a proposta agora avançada pelo CSM:

> *Isto é uma relação de duplo interesse. Os juízes vão para a política e regressam para os tribunais não apenas*

> *porque desejam isso e querem isso, mas também porque no universo da política há quem os queira lá ter. E, portanto, não sei se o parlamento quando chegar a altura da decisão abdicará dessa possibilidade facilmente".*

Para o presidente da ASJP há ainda muito a discutir sobre a forma como seria aplicada a limitação à circulação entre carreiras agora proposta, manifestando dúvidas que haja juízes interessados em ver a contagem da sua antiguidade na carreira interrompida, correndo com isso o risco de nunca atingir o topo.

O "período de nojo" de três anos proposto seria apenas "um remendo" para uma questão em que "o mais sensato" seria não se colocar a hipótese de o juiz sair para a política podendo regressar, ou se fosse convidado, o recusasse, ou, em última análise, fosse impedido pelo CSM.

> *Tudo isso era preferível a encontrar soluções na lei de proibição ou de proibição de regresso ou de estabelecimento de períodos de nojo, porque essas soluções são todas soluções de remendo e nenhuma delas é inteiramente boa e isenta de críticas", defendeu Manuel Soares.*

Segundo a proposta do CSM, os juízes que saiam para comissões de serviço terão que o fazer ao abrigo de licenças sem vencimento, e os que depois regressem ficam impedidos de exercer funções jurisdicionais durante três anos, ou seja, não podem decidir processos, ficando remetidos a cargos técnicos e de assessoria nos tribunais.

> *Ninguém quer, penso eu, ser sujeito à situação um bocadinho estranha de ser autorizado a regressar a funções, mas não poder tomar decisões. Uma pessoa fica meio-juiz? Ou é um juiz que enquanto não passar a 'contaminação do vírus' não pode mexer nos processos? Isso é uma situação um bocadinho estranha, na verdade", concluiu o presidente da ASJP.*

O CSM aprovou a 8 de março em plenário uma proposta de alteração ao EMJ, com vista a limitar a circulação de juízes entre a justiça e a política, resultado da ação do grupo de trabalho que tinha sido constituído em 2022 pelo presidente do CSM e do Supremo Tribunal de Justiça, Henrique Araújo.

De acordo com o CSM, este grupo de trabalho, presidido por Henrique Araújo, foi também constituído pelos vogais António Barradas Leitão, Inês Ferreira Leite, Jorge Raposo e Leonel Serôdio, a quem foi dada a missão de "repensar o regime legal em

vigor referente a impedimentos, incompatibilidades e comissões de serviço (judiciais e não judiciais) dos magistrados judiciais".

Henrique Araújo havia já manifestado críticas ao regime de comissões de serviço e à circulação de juízes entre a justiça e a política por ocasião da abertura do ano judicial de 2022 e numa conferência da Associação Europeia de Juízes, em abril do ano passado.

https://observador.pt/2023/03/16/lei-atual-ja-permite-fechar-as-portas-giratorias-entre-politica-e-justica-diz-asjp/ acessado em 19/05/2023

Educação básica e os desafios para a construção de um sistema articulado e a garantia dos direitos fundamentais

Mateus Silva Rocha*

Resumo

Este artigo visa compreender o diálogo necessário entre as escolas, o Estado, as famílias e sobretudo, entre os alunos. Para a produção desse estudo científico, analisámos as histórias de superação, conflitos, divergências e obstáculos à realidade de educadores e alunos do ensino básico, e, em especial as Leis garantidoras do direito educacional. Sabemos que existe inúmeras dificuldades e questões supervenientes, nas quais dificulta o trabalho dentro das grandes periferias, favelas e até mesmo nos presídios. Por isso, renovar a fé no que fazem e apoiar alunos, de dramas e vivências diversas, em uma luta pela simples crença no poder

* Licenciado (Bacharel) em Direito pelas Faculdades Santo Agostinho – FASA / AFYA, Vitória da Conquista – Bahia, Brasil. Licenciado em Letras – Língua Portuguesa pela Universidade Leonardo da Vinci - UNIASSELVI, Vitória da Conquista – Bahia, Brasil. Mestrando em Direito Judiciário pela Universidade Europeia, Lisboa. E-mail: mateus.rocha2@icloud.com

transformador da Educação, é a arma mais poderosa que nós temos. Ao decorrer do texto indicaremos pontos especiais que promete integrar os direitos humanos, acordos do Direito Internacional e os desafios para a integralização da Educação e desenvolvimento social.

Palavras-chave: Direitos Fundamentais; Educação; Sociedade e Políticas Públicas.

Educação básica e os desafios para a construção de um sistema articulado e a garantia dos direitos fundamentais

Mateus Silva Rocha

Abstract

This article aims to understand the necessary dialogue between schools, the State, families and, above all, between students. To produce this scientific study, we analyzed the stories of overcoming, conflicts, divergences and obstacles to the reality of educators and basic education students, and, in particular, the Laws guaranteeing educational rights. We know that there are countless difficulties and issues that arise, which make it difficult to work within large outskirts, favelas and even prisons. Therefore, renewing faith in what they do and supporting students, from different backgrounds and experiences, in a fight for the simple belief in the transformative power of Education, is the most powerful weapon we have. Throughout the text we will indicate special points that promise to integrate human rights, International Law

agreements and the challenges for the integration of Education and social development.

Keywords: Fundamental Rights; Education; Society and Public Policies.

Introdução

A Educação é à mola propulsora para construirmos uma sociedade melhor. Sabemos que a desigualdade social, a violência urbana e o tráfico de drogas são fatores preponderantes que afastam os adolescentes e jovens das escolas; contudo, ainda há outros inúmeros contrapontos que serão abordados ao decorrer do texto.

É de obrigação legítima dos Estados, Municípios e o Distrito Federal assegurar o direito à Educação Básica até ao acesso gratuito as universidades do Brasil. É partindo dessa visão que proponho escrever esse artigo com a finalidade de apontar a importância de investimentos e de como as instituições são capazes de mudar vidas e transformar o mundo. [554]

Educar tem sido a tarefa mais sensível e necessária até os dias de hoje. Acredita-se que o exercício mais difícil compele ao dogma "educar", é pertinente lembrar que existe inúmeras variáveis que resultam na formação do homem e não obstante, a jornada acadêmica é construída através de uma ponte socioeducativo e sociocultural.

[554] Segundo Cury (2008, p. 294), o conceito de educação básica da Constituição de 1988 é "inovador" no Brasil, tendo em vista a história brasileira de negação aos seus cidadãos do "direito ao conhecimento pela ação sistemática da organização escolar". Coerente com essa legislação, houve forte expansão de vagas, com concentração de escassez na etapa de 0 a 3 anos, o que tem instigado a luta pela garantia desse direito. Em 2005, o Supremo Tribunal Federal (STF) qualificou o direito à creche e à pré-escola como exigível coletiva e individualmente.

O devido acesso à Educação é um direito constitucional, assegurado pela Carta Magna (CRFB, 1988, art. 6° e 205°). Nesta perspectiva, imprimir este direito e proteger o livre acesso é de competência geral; famílias, o próprio Estado garantidor de direitos, os Órgãos criados pela Administração Pública e afins, são responsáveis pela promoção e efetivação da inclussão de todas as pessoas dentro das escolas públicas.

O referido dispositivo de Lei, é claro: "A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho". Para tanto, no artigo inicial do mesmo dispositivo legal, está explícito e reforçado no artigo 6° da CRFB, como direito social inerente ao ser humano.

Para Bakthin (2003, p. 261), todos os campos da comunicação humana se relacionam com a utilização da língua, desta forma, a educação é uma variação interdisciplinar. Cada campo elabora seus tipos relativamente estáveis de enunciados, os quais denominamos gêneros do discurso". (BAKHTIN, 2003, p.262 grifos do autor). No mesmo pensamento de Bakthin, indicamos a necessidade de melhorias urgentes no que tange aos programas de educação.

Ao decorrer do texto, falaremos dos principais tópicos protegidos pela Lei e a parceria com outros dispositivos. Nos últimos anos enfrentamos a Pandemia causada pelo Covid – 19, com isso, a evasão escolar aumentou gradativamente, dando números ainda maior ao sistema e afastando mais pessoas dos direitos básicos.

No que tange a educação, não foi diferente. Em 2019, tinhamos um número aproximado em 1,1 milhão, já em 2020, esse número saltou para 5,1 milhão de crianças e adolescentes sem acesso à escola. A suspensão das aulas presenciais, a falta de internet em casa, com certeza foram os principais pivores dessa evasão assustadora.

As desigualdades aumentaram e a criação de políticas públicas passou a ser uma necessidade urgente, ou, ao menos deve ser essa a preocupação do governo. Afinal, é uma Agenda de interesse social e dever de todos. Sanar parte dessas dificuldades e falicitar a entrada dessas pessoas nas instituições educacionais é uma pauta importante para os próximos anos.

Objetivos

É o objetivo central desse texto trazer as discuções da educação básica e do dever legal do Estado em garantir o livre acesso, desenvolvimento pleno e eficaz; vislumbrando um panorama entre direitos fundamentais e de como a educação impacta diretamente na vida do ser humano.

Imaginem um país com 5,6% da população sem saber ler e/ou escrever. Isto corresponde a quase 10 milhões de adolescentes e adultos. Este é um levantamento recente do IBGE (Instituto Brasileiro de Geográfia e Estátistica). Esse dado científico assusta e nos coloca em situação de maior vulnerabilidade social e menos prestígio internacional.

Se pensarmos na Agenda 2030, estamos a poucos anos para atingir o prazo estabelecido pela ONU e representantes dos Estados-Membro, e o tema Educação, é o quarto intem dessa lista. Por isso, estamos falando de algo muito maior, um contrato foi estabelecido mutuamente entre inúmeros Estados e os cidadãos de todo o mundo; estamos falando de 17 objetivos da Agenda, contudo, alguns deles, como: Erradicação da Pobreza; Erradicação da Fome; Igualdade de Gênero, e os temas 9, 10, 11 e 12, estão ligados pelo cordão umbilical da educação. Isto é, atingir o objetivo educacional e efetivar direitos, teremos um agenda quase por completa.

Uma vez que a sociedade é educada, isso causa reflexos em todos os sentidos da vida de uma pessoa. Contribui para o crescimento e articula diretamente o sistema para mudanças positivas. É um nexo que faz total diferença e não resta lacunas quanto aos resultados essenciais que precisamos para garantir o desenvolvimento social, cultural e igualdade dos direitos.

Outrossim, visamos trazer dados relacionados a diferentes vertentes da sociedade que sofrem pela ausência da educação. Além disso, há ainda outros fatores preocupantes que fazem uma somatória para inúmeros problemas a nível mundial.

É também objetivo desse trabalho salvaguardar os direitos fundamentais, sobretudo, questionar o sistema e buscar meios que possa melhorar os componentes curriculares das escolas e façam protagonistas que sonhe uma vida melhor, que buscam verdadeiramente por um futuro, e, esse futuro é hoje. É agora.

Fundamentação teórica

A escola pública é a base primordial para garantir que as oportunidades sejam iguais e direcionadas ao povo, principalmente para crianças e adolescentes das comunidades, favelas, periferias e etc., é o único caminho para reparar injustiças e melhorar uma sociedade.

A proposta educacional traçada para essas escolas, ancorada nos princípios da educação popular e da Educação de Jovens e Adultos, ao explicitar as concepções sobre o homem, sobre o mundo e sobre a educação e a produção de conhecimento, enfatiza que a educação, para ser válida, deve levar em conta a vocação ontológica do homem, e as condições nas quais vive.

A educação de qualidade que é dever do Estado e de direito de todos, sofre imensas mudanças desde a última Constituição, nas sábias palavras de Sacristán (2008, p.41)

> A educação desenvolve-se em um novo contexto [...], em uma nova realidade social que as pessoas não podem evitar. Em um primeiro nível de análise, precisamos entender que se trata de uma nova realidade constitutiva do marco em que vivemos de modo inexorável, de modo que, necessariamente, estamos nos socializando em um novo ambiente. Os indivíduos – em nosso caso, os alunos – seja qual for a orientação adotada pelas escolas, são pessoas que vivem realmente de uma ou outra maneira na sociedade, agora chamada de sociedade da informação.

De outro modo, faz-se necessário esclarecer mais um ponto de Sacristán (2008, p.41)

> Ir reconstruindo nossa visão da realidade, os discursos que mantemos para compreender o papel da educação e das escolas, seus fins na nova situação e os procedimentos de ensinar e aprender que são possíveis. Ou seja, é preciso elaborar uma nova narrativa, voltar a escrever o discurso acerca da educação; em suma, à luz de novas condições na sociedade em que nos cabe viver

As ações educacionais deve propor mudanças significativas, e ter o compromisso de transformar o mundo e as pessoas. Como afirma Freire (1983), não é apenas necessário saber que é impossível haver neutralidade da educação, mas

é preciso distinguir os diferentes caminhos. A escola é uma instituição que existe num contexto histórico de uma determinada sociedade e, para que seja compreendida, é necessário que se entenda o real valor que as salas de aula têm e o papel de cada professor.

I. Educação Básica E as Garantias Constitucionais

Inicialmente, vale destacar os artigos 205 e 206 da CRFB (Constituição, 1988): [555]

> Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho.
>
> Art. 206. O ensino será ministrado com base nos seguintes princípios: I – igualdade de condições para o acesso e permanência na escola;

Significa dizer que, é de obrigação legal do Estado garantir o acesso, a permanência e o desenvolvimento escolar em sua totalidade. Sabemos que a sociedade possui grandes responsabilidades e deve cooperar passivamente com as questões supra. Garantir que a igualdade seja efetivada e as boas e justas condições também foi uma preocupação do legislador.

Desde a última Constituição, passaram-se exatos 35 anos, e, tivemos inúmeras modificações, no entanto, os direitos fundamentais sofreram e poderão sofrer apenas melhorias, não se admite a retirada de qualquer cláusula pétrea (um direito

[555] A Constituição da República Federativa do Brasil foi muito feliz quando trouxe em seu texto os fundamentos da Educação, do dever do Estado, da sociedade e das famílias. Para garantir o acesso, a permanência e qualidade do ensino básico no Brasil. O que nos convida a pensar, o direito da educação ou à educação é essencial para o desenvolvimento social, moral e económico.

fundamental já conquistado). Ou seja, o direito a educação é protegido pela Carta Magna com forte influência do direito internacional.

No artigo 6º da CRFB, destaca um texto importante: "Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição." Ou seja, é um direito exigível.

Desde a primeira Constituição do país, já estava prevista o direito à educação, entretanto, nos últimos tempos ganhou ainda mais força. Marcada por avanços significativos e graduais. Assim, é importante fazer um paralelo entre dois temas importantes: quem é o cidadão sujeito de direito e qual é o papel do Estado para a garantia e o verdadeiro oferecimento da educação.

Ainda que de forma gradual, à educação passou por avanços históricos, de outro modo, ainda existe inúmeras camadas sociais que não gozam desse direito, parcial e/ou integral. Quando falamos de pessoas mais vulneráveis, fica ainda mais evidente a ausência de recursos e políticas públicas eficientes.

Outrossim, destaca-se, o artigo 227, também da Carta Magna:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Constituição, 1988).

O artigo 227 da CRFB elucida e ratifica mais uma vez o direito à educação, dessa vez, sendo ainda mais direto, destinando especialmente o texto da lei as crianças e adolescentes, garantindo expressamente o direito básico à educação e destacando também a sua importância. Quando se fala em profissionalização e cultura no artigo em questão faz-se presente mais uma vez a reafirmação do legislador em garantir a educação em todos os seus complexos para todos e sem distinção.

Nesta perspectiva, há um forte componente de ligação com o artigo 5º da CRFB, onde assegura a igualdade e direitos fundamentais. Sendo imprescindíveis à vida humana. São princípios norteadores da sociedade e do indivíduo. Garante uma série de direitos e protege o maior bem jurídico tutelado pelo ordenamento jurídico, qual seja, à vida.

Ainda neste caminho, o Estatuto da Criança e do Adolescente, mais conhecido como o ECA, lei brasileira de nº 8.069/90, destaca mais uma vez o direito à educação e a proteção dos preceitos fundamentais.

Em seu artigo 4º, possui a seguinte redação:

> Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária. (ECA, 1990).
>
> Art. 18-A. A criança e o adolescente têm o direito de ser educados e cuidados sem o uso de castigo físico ou de tratamento cruel ou degradante, como formas de correção, disciplina, educação ou qualquer outro pretexto, pelos pais, pelos integrantes da família ampliada, pelos responsáveis, pelos agentes públicos executores de medidas socioeducativas ou por qualquer pessoa encarregada de cuidar deles, tratá-los, educá-los ou protegê-los. (Incluído pela Lei nº 13.010, de 2014). (ECA, 1990).

Ainda no dispositivo legal do Estatuto da Criança e do Adolescente, é crucial destacar o capítulo IV, que assegura mais uma vez o direito à educação, à cultura, ao esporte e ao lazer. Para maior entendimento, segue o texto da lei em questão dos artigos 53, 53-A, 54, 55, 56, 57, 58 e 59:

> Art. 53. A criança e o adolescente têm direito à educação, visando ao pleno desenvolvimento de sua pessoa, preparo para o exercício da cidadania e qualificação para o trabalho, assegurando-se-lhes:
>
> I - igualdade de condições para o acesso e permanência na escola;
>
> II - direito de ser respeitado por seus educadores;
>
> III - direito de contestar critérios avaliativos, podendo recorrer às instâncias escolares superiores;
>
> IV - direito de organização e participação em entidades estudantis;
>
> V - acesso à escola pública e gratuita próxima de sua residência.

V - acesso à escola pública e gratuita, próxima de sua residência, garantindo-se vagas no mesmo estabelecimento a irmãos que frequentem a mesma etapa ou ciclo de ensino da educação básica. (Redação dada pela Lei nº 13.845, de 2019)

Parágrafo único. É direito dos pais ou responsáveis ter ciência do processo pedagógico, bem como participar da definição das propostas educacionais. (ECA, 1990).

Art. 53-A. É dever da instituição de ensino, clubes e agremiações recreativas e de estabelecimentos congêneres assegurar medidas de conscientização, prevenção e enfrentamento ao uso ou dependência de drogas ilícitas. (Incluído pela Lei nº 13.840, de 2019). (ECA, 1990).

Art. 54. É dever do Estado assegurar à criança e ao adolescente:

I - ensino fundamental, obrigatório e gratuito, inclusive para os que a ele não tiveram acesso na idade própria;

II - progressiva extensão da obrigatoriedade e gratuidade ao ensino médio;

III - atendimento educacional especializado aos portadores de deficiência, preferencialmente na rede regular de ensino;

IV - atendimento em creche e pré-escola às crianças de zero a seis anos de idade;

IV – atendimento em creche e pré-escola às crianças de zero a cinco anos de idade; (Redação dada pela Lei nº 13.306, de 2016)

V - acesso aos níveis mais elevados do ensino, da pesquisa e da criação artística, segundo a capacidade de cada um;

VI - oferta de ensino noturno regular, adequado às condições do adolescente trabalhador;

VII - atendimento no ensino fundamental, através de programas suplementares de material didático-escolar, transporte, alimentação e assistência à saúde.

§ 1º O acesso ao ensino obrigatório e gratuito é direito público subjetivo.

§ 2º O não oferecimento do ensino obrigatório pelo poder público ou sua oferta irregular importa responsabilidade da autoridade competente.

§ 3º Compete ao poder público recensear os educandos no ensino fundamental, fazer-lhes a chamada e zelar, junto aos pais ou responsável, pela freqüência à escola. (ECA, 1990).

> Art. 55. Os pais ou responsável têm a obrigação de matricular seus filhos ou pupilos na rede regular de ensino. (ECA, 1990).
>
> Art. 56. Os dirigentes de estabelecimentos de ensino fundamental comunicarão ao Conselho Tutelar os casos de:
>
> I - maus-tratos envolvendo seus alunos;
>
> II - reiteração de faltas injustificadas e de evasão escolar, esgotados os recursos escolares;
>
> III - elevados níveis de repetência. (ECA, 1990).
>
> Art. 57. O poder público estimulará pesquisas, experiências e novas propostas relativas a calendário, seriação, currículo, metodologia, didática e avaliação, com vistas à inserção de crianças e adolescentes excluídos do ensino fundamental obrigatório. (ECA, 1990).
>
> Art. 58. No processo educacional respeitar-se-ão os valores culturais, artísticos e históricos próprios do contexto social da criança e do adolescente, garantindo-se a estes a liberdade da criação e o acesso às fontes de cultura. (ECA, 1990).
>
> Art. 59. Os municípios, com apoio dos estados e da União, estimularão e facilitarão a destinação de recursos e espaços para programações culturais, esportivas e de lazer voltadas para a infância e a juventude. (ECA, 1990).

Em sendo assim, os artigos supracitados trazem mais uma garantia essencial as crianças, adolescentes e jovens, dando ainda mais legitimitade aos Estados e Municípios para a efetivação e proteção integral de todos os direitos já conquistados e da necessidade de investimentos cotidianos em projetos educacionais fortificados pela sociedade e também do governo.

II. Lei de Diretrizes e Bases da Educação – LDB (Lei nº 9.394/96)

A Lei de Diretrizes e Bases da Educação é a lei mais importante que se refere ao contexto educacional. Sendo esta lei aprovada em dezembro de 1996. Também conhecida como a Lei nº 9.394/96, é destinada a sociedade com o propósito de garantir a todos o devido e livre acesso a educação. Não obstante, uma educação para lá de gratuita, deve ainda ser ofertada com os requisitos de qualidade.

Foi inspirada pelo antropólogo Darcy Ribeiro (na época, Senador), que manteve suas ideias em texto amplo, sintetizado e muito bem escrito, que permite generalização e flexiblidade e com repercussões políticas. (Fagundes, 2008).

Ademais, vale destacar também que a LDB visa de forma direta garantir o pleno desenvolvimento dos professores, a sua valorização profissional e afins. Um avanço na educação de todo o país que fundamentou e deu voz a inúmeros projetos escolares traçados pelo viés socioeducativo de livre escolha de cada estado-membro e respeitando as liberdades individuais e coletivas.

Para melhor entendimento dessa tão famosa Lei, verifica a sua classificação da Educação Básica no Brasil:

1) Educação Infantil – creches (de 0 a 3 anos) e pré-escolas (de 4 e 5 anos) – É gratuita, mas não obrigatória. É de competência dos municípios.

2) Ensino Fundamental – anos iniciais (do 1º ao 5º ano) e anos finais (do 6º ao 9º ano) – É obrigatório e gratuito. A LDB estabelece que, gradativamente, os municípios serão os responsáveis por todo o ensino fundamental. Na prática os municípios estão atendendo aos anos iniciais e os Estados os anos finais.

3) Ensino Médio – O antigo 2º grau (do 1º ao 3º ano). É de responsabilidade dos Estados. Pode ser técnico profissionalizante, ou não.

4) Ensino Superior:

5) É de competência da União, podendo ser oferecido por Estados e Municípios, desde que estes já tenham atendido os níveis pelos quais é responsável em sua totalidade. Cabe a União autorizar e fiscalizar as instituições privadas de ensino superior.

Desse modo, fica evidenciado a formação na educação brasileira, sendo esta fundamental na sociedade e deve ser direcionada na sua totalidade ao povo. Asssim, há uma ordem cronológica a ser respeitada; o aluno deverá passar por esse ciclo de estudos de aproximadamente 15 anos, entre a educação ifantil até o ensino médio.

O ensino superior, por sua vez, é facultativo e relativo, sendo possível prosseguir com os estudos nas universidades privadas e/ou públicas; sendo as instituições autônomas e independentes para regular a entrada e permanência de cada estudante. De outro modo, vale salientar que, as universidades sejam elas públicas

ou privadas devem respeitar algumas regras e pressupostos para o pleno funcionamento.

A saber, o ensino superior no brasil tem duração mínima de 2, 3 e ou 4 anos, já nos cursos de Direito é obrigatoriamente o cumprimento de 10 semestres, que totalizam 5 anos, não diferente, existe regras específicas também para o curso de medicina, sendo ele ofertado por um período mínimo de 6 anos. Ou seja, são as condições de funcionamento dos cursos do ensino superior no Brasil. Geralmente, regulados pelas portarias de autorização do MEC – Ministério da Educação, orgão máximo da União.

III. Declaração Universal dos Direitos Humanos e outros Tratados Internacionais

Outrossim, na Declaração Universal dos Direitos Humanos, temos um artigo especial que trata desse tema, a comunidade internacional, entendeu ser matéria sensível e necessária para todo o mundo, é tão verdade que, destinou um artigo para a proteção e efetivação da educação.

No artigo 26 da Declaração em questão, destaca-se a seguinte redação:

> *"1. Todos os seres humanos têm direito à educação. A educação será gratuita, pelo menos nos graus elementares e fundamentais. A educação elementar será obrigatória. A educação técnico-profissional será acessível a todos, bem como a educação superior, esta baseada no mérito. 2. A educação será orientada no sentido do pleno desenvolvimento da personalidade humana e do fortalecimento do respeito pelos direitos humanos e pelas liberdades fundamentais. A educação promoverá a compreensão, a tolerância e a amizade entre todas as nações e grupos raciais ou religiosos, e coadjuvará as atividades das Nações Unidas em prol da manutenção da paz."*

Reconhecida em quase todo o mundo, a Declaração Universal dos Direitos Humanos tem grande influência no cumprimento das normas internas de cada país; zelar pela paz, prosperidade, desenvolvimento, saúde, segurança mundial e outros pontos que estão na Agenda internacional, são compromissos sérios e importantes para melhorar o mundo.

Assim sendo, existe outros dispositivos que interfere diretamente nesse sistema de inclusão de normas protetoras desse direito tão importante. O Pacto Internacional de Direitos Econômicos, Sociais e Culturais (PIDESC), aprovado pela Assembléia Geral da ONU em 16 de dezembro de 1966. É apenas mais um dos muitos conteúdos que foram criados e aprovados pela Camada Protetora dos direitos fundamentais internacionais.

Mais do que educar, pensar no modus operacional do Estado, as suas mazelas e gerência organizacional, é uma saída fundamental para o avanço e pleno acesso dos direitos fundamentais e sociais. Para Arroyo (2011, p.25)

> As políticas neoliberais, sua ênfase no treinamento e no domínio de resultados voltam a expatriar a educação dos seus territórios, as escolas, os currículos e a docência. Nossa bandeira de luta desde os anos de 1980, educação como direito sai do discurso. Os termos direito, educação (quando ainda não se usam) são reduzidos a termos como domínio de competências ou mostram quantificação dos resultados.

A base de qualquer sociedade é a educação, o mundo se reconstrói através dela. Há inúmeros pesquisadores que já articulavam e debatiam acerca do contexto escolar. Contudo, no século XVIII começou a surgir as primeiras escolas. Johann Heinrich Pestalozzi, educador suiço e criador de um sistema de aprendizagem e ensino voltado para os alunos, deu origem à escola do século.

No documentário "Nunca me Sonharam", podemos observar com claresa a responsabilidade que os professores tomam para si, enfrentam o sistema com garra e decididos a ajudar aquelas crianças e adolescentes que nunca foram "sonhadas por ninguém."

Assim, compreende que, o Estado em sua maior parte do tempo, desintegra da sociedade inúmeros grupos; porque estamos falando de uma instituição que generaliza e ao mesmo tempo classifica, há pessoas que não tem acesso aos seus direitos básicos, na verdade, são milhões de pessoas. E, muitas vezes os líderes políticos fecham os olhos para essa realidade.

IV. Princípio da Dignidade da Pessoa Humana

Sempre que estivermos falando de um ser humano devemos pensar nos princípios norteadores, que são a base de um estado democrático de direito. A dignidade humana está intrisecamente ligada com o desenvolvimento histórico do mundo, as suas necessidades de reconhecer os direitos para todos e sem distinção alguma.

E, é, pesando nisso que o Estado precisa garantir o livre desenvolvimento, um país mais justo e melhor para viver. Nesta perspectiva, no final do século XVIII, Immanuel Kant inicia-se a construção do conceito de dignidade humana, fazendo assim uma abordagem crucial que prospera até os dias de hoje. Kant sustenta que:

> [...] um ser humano considerado como uma pessoa, isto é, como o sujeito de uma razão moralmente prática, é guindado acima de qualquer preço, pois como pessoa (*homo noumenon*) não é para ser valorado meramente como um meio para o fim de outros ou mesmo para seus próprios fins, mas como um fim em si mesmo, isto é, ele possui uma dignidade (um valor interno absoluto) através do qual cobra respeito por si mesmo de todos os outros seres racionais do mundo.

A discussão acerca da dignidade humana pondera desde ao nascimento da pessoa até à sua morte, em sentido estrito, é assegurar que independentemente de cor, raça, religião, sexo e etc., a pessoa tenha os seus direitos resguardados, assim como preza na Carta Magna de 1988 da República Federativa do Brasil e dentre outros diplomas legais.

É extremamente necessário reconhecer os direitos fundamentais. Quando estes estão em conflito, estima-se que mais pessoas estarão sujeitas a terem seus direitos cerceados pela inversão do Estado de punir e combater a criminalidade e afins, por esta razão deve-se buscar meios para lhes assegurar seus direitos e se compreender que:

> Os detentos não são meus amigos, mas não é necessário ser meu amigo para que eu reconheça, a cada um, seus direitos. O direito não é dado por compaixão, mas porque é um direito. Ele não necessita de explicação alguma. É porque decidimos viver em sociedade, reconhecendo a cada um os mesmos direitos, que esta exigência moral se torna uma exigência social, jurídica. Não se trata de bem ou mal no reconhecimento dos direitos de cada um. (MAEYER, 2013, p. 48-49)

É dever constitucional zelar pela efetivação dos direitos humanos e a promoção de políticas públicas inclusivas e preponderantes. Que sejam capazes de interagir com o núcleo "social" e observação e cumprimento do que diz o Ordenamento Jurídico, bem como, observar os Tratados Internacionais e a matriz de direitos humanos no âmbito internacional.

V. Direito Penal e Educação

A educação é fundamental e importante na sociedade, sabemos que é através dela que, os direitos são verdadeiramente protegidos. O homem busca os seus direitos de acordo com as suas necessidades; os grupos sociais se transformam dia após dia. Quando passam pelo crivo educacional e compreendem os seus direitos, estes coletivos se desenvolvem e atigem maturidade social. Para tanto, Teixeira explica que:

> O direito à educação faz-se um direito de todos, porque a educação já não é um processo de especialização de alguns para certas funções na sociedade, mas a formação de cada um e de todos para a sua contribuição à sociedade integrada e nacional, que se está constituindo com a modificação do trabalho e do tipo de relações humanas. (TEIXEIRA, 1996, p. 60).

Ou seja, é necessário garantir o livre acesso de aprendizado para que as pessoas estejam preparadas para o mundo, as suas significativas mudanças e garantias de direitos sociais, através desses mecanismos, o homem automaticamente se transforma e reduz as chances de delinquir na esfera social.

Segundo Cury (2002), impõe ao Estado o dever de oferecê-la gratuitamente, para que seja acessível a todos os cidadãos. Uma vez que, o homem aprende viver na sociedade e compreende as suas necessidades e o seu papel no mundo, diminui as chances do indivíduo delinquir; ainda que este não seja o objeto desta pesquisa, é necessário fazer esse paralelo com o direito penal.

Destarte, o agente que se educa, é primariamente privilegiado, isto é, possui outras vertentes, não o impede de praticar qualquer tipo de crime, mas leva a pessoa para outra atmosfera, sendo este educado pelo sistema, possui maiores chances de sobressair; considerando os jovens e adolescentes das grandes periferias.

Quando buscamos lidamos com o instituto do direito penal, é possível perceber como o Estado é ineficiente nesta matéria, como forte exemplo temos a política do encarceramento em massa. Visando amenizar a criminalidade e superlotar os presídios de todo o país.

Assim, pondera-se um fator infeliz, temos um país que constrói mais penitenciárias do que escolas públicas. Falhamos miseravelmente. As instituições falharam antes de tudo. O seu dever legal de zelar pelo desenvolvimento, bem como o livre acesso as escolas e investimentos de políticas públicas capazes de elevar o nível educacional do Brasil.

Seria utopia pensar em um Estado sem criminalidade, mas observa-se que somos totalmente capazes de viver evitando crimes e com mais vontade de estudar, traçar metas de futuro e pensar em como melhorar de vida. Isto é, somos parte integral do meio de onde viemos, mas se temos um governo que se preocupa com o crescimento e a igualdade de todos, com certeza teremos mais chances de viver a parte boa da vida.

Agraciados com uma educação forte e recorrente, o indivíduo é levado a crescer mesmo que este último não queira, mas sempre terá em si o viés do *bom homem* e dos principios sociais. Cresceu com uma base forte e fundamentada em valores.

Certamente, o direito penal não baterá sempre na porta das pessoas que moram em favelas e são negligenciados pela administração estatal, serão fortemente afetados pelo poder transformador que existe na educação; livros contam histórias, pessoas escrevem histórias e outras mais lêem estas mesmas histórias. De outro mdo, há que se falar também nas pessoas que entram definitivamente para a história por usarem os livros e a educação em fase do próximo e do seu próprio benefício.

Teremos chances de combater injustiças e reparar danos históricos, trata-se de um povo que não marginalizado pelo o sistema como vem sendo nos últimos tempos. É uma história que merece um capítulo final diferente, sabemos que as instituições deverão ser fortalecidas com a crença de credibilidade nos direitos fundamentais e na exclusão de culpa de agentes inocentes em todo o país.

São os sonhos e objetivos de uma nação que por muitas vezes foi silenciada, mas hoje, no presente século, escrevem novos roteiros e se transformam por novas ideias e posicionamentos. São autores das suas próprias escolhas.

O direito penal perde a sua força por um ponto forte e uma corrente do bem; educar a sociedade é mais do que pensar no cumpriemnto das políticas educacionais, visa um objetivo ainda maior, trazer a dignidade humana, afastar os preconceitos que enfrentam as milhões de pessoas no Brasil que um dia foam privadas da educação, que sabemos todos, ser um direito fundamental.

VI. O Seriado de Televisão "Segunda Chamada" e à Deficiência de Recursos nas Escolas Públicas

Neste tópico, faremos um link com à série de televisão "Segunda Chamada" (Globoplay, 2022), com a realidade escancarada dos últimos anos no cenário escolar. Destaca-se a real condição dos grandes centros brasileiros, os problemas causados pela deficiência de estrutura educacional, a falta de investimentos por parte do Poder Público e dentre outras mazelas da sociedade, dessa forma, esse seriado foi citado aqui por observar inúmeros problemas nas instituições e trazer ao público uma discussão iminente e centralizada na marginalização da educação básica.

Diante dos desafios atuais interpostos à educação de distintos níveis, é premente retomar o significado, o sentido, as teorias e as possibilidades de desenvolvimento da prática pedagógica por meio de metodologias ativas, sendo assim, é necessário levar a educação para esses jovens (homens, mulheres, crianças e adolescentes).

No tocante à educação de jovens e adultos, temos um alto número de evasão escolar; são muitas as pessoas que precisam trabalhar e estudar simultaneamente. Com isso, muitos deles precisam no meio do caminho desistirem dos seus sonhos para garantir que tenham comida na mesa, acesso à água potável e etc., são estes e outros fatores que afastam grande parte da população de inúmeros estados brasileiros das escolas.

Ainda em consenso com a série de tv, que retrata um drama real e presente, temos que falar da ausência de docentes, equipamentos eletrônicos e infraestrutura para assegurar aos alunos um ambiente seguro e capaz de proporcionar metodologias ativas e inovadoras, tomando a atenção dos alunos para concluirem as etapas e posteriormente alcançar novos objetivos – o ensino superior, por exemplo.

Métodos

Nesta pesquisa usamos a metodologia de tipo documental, com o desenho qualitativo e o escopo exploratório. Visando compreender as diferentes faces da educação e formação sociocultural. Determinando pontos lineares entre as instituições educacionais e programas sociais de cunho científico.

Outrossim, de forma interdisciplinar professores, alunos e familiares contribuiram para esta pesquisa; após a leitura e observação de inúmeros depoimentos de pessoas que acreditam na educação e defendem as políticas públicas. Por meio da intervenção do Estado, dos investimentos sérios e reiterados, teremos um cenário diferente para os próximos anos.

Assim sendo, estamos a falar de uma agenda necessária, esta pauta não pode ficar na gaveta, é importante, séria e urgente. Outrora, Paulo Freire já defendia: "Quando a educação não é libertadora, o sonho do oprimido é ser o opressor." "Se a educação sozinha não transforma a sociedade, sem ela tampouco a sociedade muda." "Ensinar não é transferir conhecimento, mas criar as possibilidades para a sua própria produção ou a sua construção."

Por esta razão, buscamos nos livros e na realidade atual do Brasil e do mundo alguns dos diversos recursos que temos para falar de um tema delicado e denso. Afinal, não existe outro caminho que se leva a ciência e evolução humana se não vier da educação, do senso de pesquisa e da vontade de transformar o mundo.

Considerações Finais

A sociedade é formada por organizações, sendo estas últimas capazes de desenvolver técnicas e meios alternativos para incluir todas as pessoas dentro de um só núcleo social, indo além das diferenças entre pessoas. Busca-se um meio eficaz e valorativo para alcançar resultados promissores. No que tange a educação, tivemos grandes conquistas e avanços. Mas, ainda há muito para melhorar.

Isto é, em matéria de investimentos e a criação de políticas públicas, destaca-se a necessidade de introduzir um sistema novo e completo onde os jovens sejam inseridos nas escolas de forma integral, respeitando as diferentes camadas de um país que soma mais de 200 milhões de pessoas; existe um caminho que acreditamos e defendemos para levar o nosso povo ao mais alto nível de desenvolvimento.

Como já citado anteriormente e reiterando nas considerações finais, a criação de políticas públicas e investiementos sérios ajudará na transformação do país e do mundo. Faremos uma história diferente; não apenas com livros e canetas, mas também com muito trabalho, arte, cultura, segurança social e a proteção dos direitos humanos, sobretudo, aqueles que são fundamentais à vida.

Por fim, entendemos que as escolas contribuem integralmente para o livre desenvolvimento, com os estudos científicos e também para o progresso do mundo em todas as suas esferas. É crucial destacar nesta fase final do artigo a importância de buscar por meios reais de acelerar a criação de políticas públicas educacionais e propor medidas eficazes para construir mais escolas e ponderar a qualidade da educação ofertada para a nação brasileira.

Referências

Aladio Anastacio Dullius, Jackson André Müller Hartmann: Âmbito Jurídico. ***Análise do Sistema Prisional Brasileiro.*** Disponível em: http://www.ambito- -juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_ id=10878. Acesso em 25 de Outubro de 2023.

BRASIL. [Constituição (1988)]. ***Constituição da República Federativa do Brasil de 1988.*** Brasília, DF: Presidente da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 30 de outubro de 2023.

BRASIL. Lei nº 9.394, de 20 de Dezembro de 1996. ***Dispõe sobre a Lei de Diretrizes e Bases da Educação Nacional [...].*** Brasília, DF, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007- 2010/2009/Lei/L11947.htm. Acesso em: 31 out. 2023.

BRASIL. Lei nº 8.069, de 13 de Julho de 1990. ***Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências [...].*** Brasília, DF, [2009]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007- 2010/2009/Lei/L11947.htm. Acesso em: 31 out. 2023.

CANOTILHO, J. J. Gomes. ***Direito constitucional e teoria da Constituição.*** 7. ed. reimp. Coimbra: Almedina, 2017.

COSTA, Gabriela Gomes. ***Justiça restaurativa no Brasil: uma possibilidade.*** 2009. 63 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2009.

DIMOULIS, Dimitri; MARTINS, Leonardo. ***Teoria geral dos direitos fundamentais.*** São Paulo: Atlas, 2014.

FERREIRA FILHO, Manoel Gonçalves. ***Direitos humanos fundamentais.*** São Paulo: Saraiva, 2010.

GARCIA, Maria. ***"Educação, problema básico da Democracia": o Estado Federal e a atuação dos conselhos educacionais.*** Revista de direito educacional, nº 1, ano 1. São Paulo: Revista dos Tribunais, jan./jun., 2010.

LIBÂNEO, José Carlos; OLIVEIRA, João Ferreira de. TOSCHI, Mirza Seabra. ***Educação escolar: políticas, estrutura e organização.*** São Paulo: Cortez, 2012.

LOCKE, John. ***Pensamientos sobre la educación.*** Madrid, Espanha: Akal, 1986.

NUNES JR., Vidal Serrano. ***A cidadania social na Constituição de 1988: estratégias de positivação e exigibilidade judicial dos direitos sociais.*** São Paulo: Verbatim, 2009.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos, 1948.** Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 20 de out. 2023.

RANIERI, Nina Beatriz Stocco. **O direito educacional no sistema jurídico brasileiro. *Justiça pela qualidade na educação.*** São Paulo: Saraiva, 2013.

Organização Associação Brasileira de Magistrados, Promotores de Justiça e Defensores Públicos da Infância e da Juventude. Todos pela Educação, pp. 55-103.

Direitos Fundamentais e a Proteção de Dados

Leonel do Rosário Filipe Salgueiro

Resumo
Os direitos fundamentais são conquistas que garantem aos indivíduos uma série de direitos e liberdades básicas, considerados essenciais para a dignidade humana e o pleno desenvolvimento da personalidade. Eles, são universalmente reconhecidos e protegidos por diversas normas jurídicas, incluindo as Constituições dos Estados. Entre os direitos fundamentais, consagrados a luz da Constituição portuguesa, encontra-se o direito à privacidade, que inclui a proteção de dados pessoais. Esse direito, assegura que as pessoas tenham controle sobre as informações que são coletadas sobre elas, bem como, a forma como esses dados são utilizados e compartilhados. A proteção de dados, por sua vez, consiste em um conjunto de medidas e garantias jurídicas que visam resguardar a privacidade das pessoas e a segurança das informações que lhes dizem respeito. Isso, envolve desde a coleta e o armazenamento adequados dos dados pessoais até a sua utilização de forma responsável e segura. Essa proteção é especialmente relevante no contexto digital, em que a coleta e o processamento de dados ocorrem de forma cada vez mais intensiva e abrangente. O avanço da tecnologia trouxe consigo novos desafios como, a necessidade de equilibrar a inovação e a conveniência, proporcionadas pelo uso dos dados com o respeito à privacidade e aos direitos fundamentais dos indivíduos. Assim, a proteção de dados tornou-se um tema central no campo jurídico, sendo objeto de regulamentações específicas em diversos países e regiões, bem como, de instrumentos internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia. O objetivo é garantir que as pessoas tenham o máximo

controle sobre as suas informações pessoais, bem como promover a transparência e a prestação de contas por parte das organizações que coletam e processam esses dados.

Palavras-chave: Direitos Fundamentais. Direitos Humanos. Proteção de Dados. Constituição da República Portuguesa.

Direitos Fundamentais e a Proteção de Dados

Leonel do Rosário Filipe Salgueiro

Abstract
Fundamental rights are achievements that guarantee individuals a series of basic rights and freedoms, considered essential for human dignity and the full development of the personality. They are universally recognized and protected by various legal norms, including State Constitutions. Among the fundamental rights is the right to privacy, which includes the protection of personal data. This right ensures that people have control over the information that is collected about them, as well as how this data is used and shared.
Data protection, in turn, consists of a set of measures and legal guarantees that aim to protect people's privacy and the security of information that concerns them. This involves everything from the appropriate collection and storage of personal data to its responsible and safe use. This protection is especially relevant in the digital context, where data collection and processing occurs in an increasingly intensive and comprehensive manner. The advancement of technology has brought with it new challenges, such as the need to balance the innovation and convenience provided by the use of data with respect for the privacy and fundamental rights of individuals. Thus, data protection has become a central topic in the legal field, being the subject of specific regulations in different countries and regions, as well as international instruments, such as the European Union's General Data Protection Regulation. The objective is to ensure that people have maximum control over their personal information, as well as to promote transparency and accountability on the part of the organizations that collect and process this data.

Keywords: Fundamental Rights. Human Rights. Data Protection. Constitution of the Portuguese Republic.

Abreviaturas

ART. - Artigo

C.C. – Código Civil Português

CDFUE. - Carta dos Direitos Fundamentais da União Europeia

CRA. – Constituição da República de Angola

CRP. – Constituição da República Portuguesa

DH. – Direitos Humanos

RGPD. – Regulamento Geral de Proteção de Dados

Introdução

Os direitos fundamentais são considerados como a base de qualquer sociedade democrática e, estão presentes em praticamente todas as constituições do mundo.

São direitos inalienáveis e universais e que garantem a dignidade e a liberdade de cada indivíduo.

Esses direitos estabelecem os limites para o poder do Estado, protegendo a integridade física, moral e psicológica das pessoas, além de assegurar condições mínimas para que elas possam exercer plenamente sua cidadania.

Existem diferentes categorias de direitos fundamentais, como os direitos civis e políticos, como o direito à vida, liberdade de expressão e participação política; os direitos econômicos, sociais e culturais, que garantem o acesso à habitação, saúde, educação e trabalho; e os direitos de grupos específicos, como das crianças, mulheres, idosos, minorias étnicas e religiosas.

Esses direitos devem ser garantidos e protegidos pelos Estados, que têm a responsabilidade de criar leis e políticas públicas que respeitem e promovam os direitos fundamentais de todos os cidadãos.

1. Natureza e Conceito dos Direitos Fundamentais. Breves Considerações

Os direitos fundamentais fazem parte do leque de situações jurídicas de bastante complexidade, tanto ao nível conceitual como ao nível prático[556]. Os direitos fundamentais, podem ser entendidos na sua essência como aqueles direitos e liberdades que as pessoas detêm pelo simples facto de serem dotadas de caráter humano, possuindo uma natureza essencial para garantir a existência do indivíduo; estando, porém, intimamente ligado à uma visão de igualdade e de liberdade dos indivíduos[557].

Segundo Jónatas Machado (1996), a primeira tese [dos direitos fundamentais] de inspiração preponderantemente lockeana e kantiana, corresponde ao pensamento de autores como Rawls, Dworkin, Richards, e outros que, partindo de teses neo-contratualistas ou de um discurso filosófico político-moral, procuram identificar um conjunto de direitos fundamentais deduzidos a partir de princípios de justiça ou de prerrogativas morais da personalidade, afirmando a sua inegociável prioridade na ordenação da comunidade política.

---

[556] Oliveira, Gomes & Santos: Os Direitos Fundamentais em Timor-Leste. 2015, p.29.

[557] *Idem*

Os direitos fundamentais, podem ser, muitas das vezes, definidos pela sua finalidade: proteger direitos e liberdade das pessoas, aplicáveis essencialmente na relação pessoa-Estado.

Os direitos fundamentais são o resultado de um processo de constitucionalização. Canotilho (2003) aborda este processo como "a incorporação de direitos subjetivos do homem em normas formalmente básicas, subtraindo-se o seu reconhecimento e garantia à disponibilidade do legislador originário"[558]. Jorge Miranda (1999) considera que os direitos fundamentais são entendidos como "os direitos ou as posições jurídicas subjetivas das pessoas enquanto tais, individual ou institucionalmente consideradas, assentes na Constituição"[559].

A conceptualização dos direitos fundamentais deverá ser fortalecida com uma apreciação das suas principais caraterísticas, classificações e funções, na medida em que nem o seu conceito filosófico nem o positivista fornecem uma compreensão exaustiva a seu respeito.

2. Fontes dos Direitos Fundamentais

Para melhor se compreender, acerca dos direitos fundamentais, pensamos ser de suma importância fazer uma análise das suas fontes normativas.

Fontes do Direito, é tudo que dá origem ou produz o Direito. Ou seja, as formas de como a norma jurídica se manifesta[560].

Em seu sentido técnico-jurídico, podem ser definidas como os modos de formação e revelação das normas jurídicas em um determinado ordenamento jurídico.

Tradicionalmente, são enumeradas três fontes do Direito: a lei, a jurisprudência, e a doutrina. Note-se que a Constituição portuguesa não reconhece expressamente o costume como fonte de Direito, tal como acontece por exemplo com a sua homóloga Timorense no seu art. 2.º n. 4 e a também a homóloga angolana no seu art. 7.º CRA. As diferentes fontes são ainda classificadas como fontes imediatas ou mediatas. As fontes imediatas são aquelas que criam normas jurídicas, enquanto as fontes mediatas ocupam uma função de contribuição para a formação das normas jurídicas, sem representarem, propriamente, uma norma de valor legal.

---

[558] Oliveira et al. 2015, p30. Apud: Gomes Canotilho, Direito Constitucional E Teoria Da Constituição, p.378.

[559] Oliveira et al. 2015, p30. Apud: Jorge Miranda, Direitos Fundamentais: Introdução Geral. 1999, p.11.

[560] Agostinho, Adlezio: Curso de Direito Constitucional. 2019, p.53.

No âmbito geral das fontes de Direito em Portugal, as leis são as principais fontes imediatas do Direito[561].

As leis e outros diplomas legislativos representam instrumentos importantes como fontes tanto de normas de direitos fundamentais como de normas necessárias para a aplicação destes.

Normas positivadas em leis ordinárias podem estabelecer normas de direitos fundamentais. Tal é fruto da abertura do sistema dos direitos fundamentais estabelecida no artigo 16.º n.1 da CRP[562].

Quando os direitos fundamentais são previstos nas leis, possuem um carácter extra constitucional e são classificados como *direitos só materialmente fundamentais*[563]. Considerando esta abertura do sistema, deparamo-nos com a difícil tarefa de identificar quais as normas previstas em leis ordinárias que podem ser consideradas como direitos fundamentais (em sentido só material) e quais aquelas que não podem ser consideradas como tal.

As leis e outros diplomas legislativos são de suma importância para a implementação dos direitos fundamentais. A própria Constituição faz referência à necessidade da regulamentação por lei de vários padrões de direitos fundamentais. Como são os casos do direito à manifestação art. 45.º, do direito à greve art. 57.º, direito à assistência social, direito à saúde art. 64.º, e outros. As leis podem ainda estabelecer o sistema para a implementação de um certo direito fundamental, assim como as instituições responsáveis para a sua execução. Por exemplo, o direito fundamental ao sufrágio previsto no art. 49.º n.1 da CRP. É implementado no contexto das eleições, através de uma gama de atos legislativos, nomeadamente leis eleitorais, legislação que estabeleça e regule órgãos da administração eleitoral, criminalize atos que colidam com o gozo deste direito e que crie a base legal para a constituição de partidos políticos.

As normas de direitos fundamentais podem ser encontradas nas diferentes fontes do Direito internacional público, sendo os tratados e os costumes as suas principais fontes, onde passam a ser chamados de Direitos Humanos, em que a ideia primordial, passa por garantir o respeito pela paz e pela segurança internacional,

---

561 Conforme dispõe o n.º 1 do artigo 1.º do C.C, "São fontes imediatas do direito as leis e as normas corporativas".

562 Segundo o qual "Os direitos fundamentais consagrados na Constituição não excluem quaisquer outros constantes das leis...". O que nos permite dizer que, embora os direitos fundamentais, sejam essencialmente os previstos expressamente no texto constitucional, podem também, ser reconhecidos como fundamentais, outros direitos que não estejam descritos de forma explícita na Constituição, ou seja, que estejam de forma implícita.

563 Oliveira et al.: Os Direitos Fundamentais em Timor-Leste. 2015, p55.

cujo primeiro e indispensável passo seria o respeito pelos DH na ordem interna de cada Estado.

O ponto de partida para a identificação das fontes do Direito ao nível internacional é o artigo 38.º n.1 do Estatuto do Tribunal Internacional de Justiça, que é geralmente considerado pela doutrina, como o elenco tradicional das fontes do Direito internacional[564]. O artigo 38.º n. 1 do Estatuto do Tribunal Internacional de Justiça identifica cinco fontes do Direito internacional a ser aplicado por este próprio tribunal: as convenções internacionais, o costume internacional, os princípios gerais do Direito, as decisões judiciais e a doutrina. Às cinco fontes identificadas no Estatuto do Tribunal Internacional de Justiça é adicionada uma sexta fonte: os atos das organizações internacionais[565].

As convenções ou tratados internacionais, os costumes e o *jus cogens* são fontes imediatas de Direito, sendo os princípios gerais do Direito, ao passo que as decisões judiciais, a doutrina e as decisões de organizações internacionais fontes mediatas de Direito.

Apesar de serem encaradas como diferentes fontes de Direito internacional, o direito convencional, o costume, os princípios gerais do Direito, as decisões judiciais, a doutrina e as decisões de organizações internacionais não atuam de forma isolada.

Sobre este assunto, Jorge Miranda[566] explica que "As categorias de fontes surgem em abstrato com suficiente autonomia. Em concreto, são interdependentes e as normas através delas criadas entrelaçam-se sistematicamente, sem prejuízo de consideração de zonas diferenciadas (direito internacional universal e direito internacional regional, direito das Nações Unidas, direito europeu dos direitos dos homens, (…) etc.)."

3. O Direito à Proteção de Dados

A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da assim chamada sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática e da ampla digitalização que já

[564] Oliveira et al.: Os Direitos Fundamentais em Timor-Leste. 2015, p59.

[565] Idem.

[566] Oliveira et al. 2015, p60. Apud: Jorge Miranda, Curso de Direito Internacional Público, 2009, 44.

assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica, política, cultural contemporânea no Mundo[567].

A Constituição portuguesa de 1976 contempla no seu artigo 35.º o direito à proteção de dados como um direito fundamental em Portugal. Além disso, Portugal também está vinculado ao Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, que assegura a proteção dos dados pessoais de todos os cidadãos na União Europeia.

O RGPD estabelece os princípios e as regras para o tratamento de dados pessoais, garantindo um nível elevado de proteção dos direitos e liberdades dos indivíduos.

O RGPD é uma legislação criada pela União Europeia em 2016, com o objetivo de proteger a privacidade e os dados pessoais dos cidadãos europeus. Entrou em vigor em 25 de maio de 2018 e substituiu a Diretiva de Proteção de Dados de 1995.

O Regulamento Geral da Proteção de Dados, tem por objetivo nos termos do seu art. 1.º estabelecer o conjunto de regras sobre como as organizações devem coletar, armazenar, processar e proteger os dados pessoais das pessoas. Ele se aplica a todas as empresas e organizações que operam dentro da União Europeia, bem como aquelas que oferecem bens ou serviços aos cidadãos europeus.

Algumas das principais mudanças trazidas pelo RGPD incluem a ampliação dos direitos dos indivíduos em relação aos seus dados, como o direito ao acesso, retificação e exclusão dos dados 13.º n. 2 b); a obrigatoriedade de obter consentimento claro e específico para a coleta e uso dos dados pessoais 6.º n. 1 a); a necessidade de implementar medidas de segurança adequadas para proteção dos dados 5.º n. 1 f); e a implementação de um regime de sanções rigoroso para as empresas que não estiverem em conformidade com as regras do RGPD.

O RGPD também introduziu a figura do Encarregado de Proteção de Dados, que é responsável por garantir a conformidade com o regulamento dentro de uma organização.

De um modo geral o RGPD é uma legislação que busca garantir a proteção dos dados pessoais dos cidadãos europeus, promovendo maior transparência, controle e segurança no uso dessas informações pelas empresas.

No âmbito da Carta dos Direitos Fundamentais da União Europeia, o seu art. 8.º trata do direito à proteção de dados pessoais. Estabelecendo que todas as pessoas têm o direito de proteção das informações que lhes dizem respeito,

[567] SARLET, Ingo. O Direito Fundamental à Proteção de dados pessoais na Constituição Federal Brasileira de 1988. ***Privacy and Data Protection Magazine,*** p.12. 2021.

especialmente em relação ao tratamento desses dados por parte das instituições e órgãos da União Europeia.

Baseando-se no princípio de que a proteção dos dados pessoais é um direito fundamental e deve ser respeitada em todas as etapas do seu tratamento. Isso inclui a coleta, o armazenamento, a transferência, a divulgação e o acesso a esses dados.

Para garantir essa proteção, o art. 8.º estabelece que o tratamento de dados pessoais deve ser feito de forma transparente, justa e com base no consentimento do titular dos dados. Além disso, as pessoas têm o direito de acessar, retificar e apagar seus dados pessoais, bem como o direito de restringir o seu tratamento, e determina ainda, que os dados pessoais devem ser processados para fins específicos e legítimos, e devem ser tratados de forma adequada, pertinente e limitada ao necessário para a finalidade do seu tratamento. A segurança dos dados pessoais também é uma preocupação, e medidas técnicas e organizacionais adequadas devem ser adotadas para proteger essas informações.

Podemos assim ver através da CDFUE refletida a importância atribuída à proteção de dados pessoais na União Europeia, e também e o seu alinhamento com o Regulamento Geral de Proteção de Dados, que estabelece normas específicas sobre o tratamento de dados pessoais na União Europeia.

Ainda no âmbito do Tratado da União Europeia, que define os objetivos da UE, os princípios em que se baseia e os poderes atribuídos às suas instituições, a proteção de dados é uma área específica do direito abordada e que merece a sua atenção.

O TUE protege os direitos à privacidade e proteção de dados dos indivíduos na UE por meio do RGPD e da atuação das autoridades de proteção de dados. Essas regulamentações buscaram harmonizar as leis de proteção de dados nos Estados membros da UE e garantir um alto nível de proteção para os cidadãos europeus.

Conclusão

Os direitos fundamentais são considerados a base de qualquer sistema jurídico democrático e têm como objetivo proteger a dignidade humana e garantir a liberdade, igualdade e segurança de todas as pessoas. Esses direitos são reconhecidos e protegidos em diversas constituições e tratados internacionais.

No contexto da proteção de dados, os direitos fundamentais têm um papel fundamental. A proteção de dados é um aspeto essencial da privacidade individual e está relacionada à capacidade de controlar as informações pessoais, limitar seu uso e garantir sua segurança.

Em muitos países, há legislação específica que estabelece os princípios e diretrizes para a proteção de dados pessoais, como o consentimento prévio do titular dos dados, o dever de informação, a finalidade específica para a coleta dos dados e o direito de acesso e retificação.

No entanto, a proteção de dados não é apenas um direito individual, mas também uma preocupação social. Neste sentido, as autoridades competentes têm um papel importante em regulamentar e fiscalizar o cumprimento das leis de proteção de dados, especialmente diante do avanço das tecnologias da informação e comunicação.

Dessa forma, é possível concluir que os direitos fundamentais e a proteção de dados são áreas interdependentes do direito, que buscam garantir o respeito à liberdade, privacidade e segurança das pessoas em um mundo cada vez mais conectado. A adoção de legislação adequada, aliada à conscientização e à responsabilidade social, são fundamentais para assegurar o equilíbrio entre a inovação tecnológica e a proteção dos direitos individuais.

Referências bibliográficas

OLIVEIRA, Bárbara. Gomes, Carla & Santos, Rita. Os Direitos Fundamentais em Timor Leste: Teoria e Prática. 1ª. Ed. Coimbra. Coimbra Editora. 2015. ISBN 978-989-20-5236-6.

AGOSTINHO, Adlezio. Curso de Direito Constitucional. 1ª. Ed. AAFDL Editora. 2019.

SARLET, Ingo. O Direito Fundamental à Proteção de dados pessoais na Constituição Federal Brasileira de 1988. Privacy and Data Protection Magazine. ISSN 2184-920X. 2021. P. 12-50.

Legislação Consultada

Constituição da República Portuguesa. 2022. 3ª. Ed. AAFDL Editora: Lisboa.

Código Civil Português. 2017. AAFDL Editora: Lisboa.

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2016/C 202/02).

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016.

Proteção de dados ontem, hoje e amanhã

Paulo Alexandre Dias da Silva Constantino Teles[568]

Resumo

O presente relatório versa sobre a proteção de dados num escopro temporal, ou seja, desde os primórdios até aos possíveis desafios do futuro. O nosso objetivo é entender melhor como surgiu a proteção de dados, a sua finalidade, o impacto que tem nas nossas vidas e olhar numa perspetiva de dedução para os possíveis problemas que possam surgir no futuro. Entendemos que esta questão tem uma relevância sem igual para o estudo do Direito, porque, aparentemente estamos a falar de um ramo do direito novo, mas, na verdade não é e a sua evolução tem sido tão rápida quanto a velocidade da luz. Neste contexto, esta pesquisa foi feita com base numa realidade global, pese embora o ponto de partida foi a União Europeia e também por acreditamos que este tema é de certo modo uma questão atual e permanente, pois, é notório o desenvolvimento, crescimento e a dependência do ser humano pelas novas tecnologias. Outrossim, também temos em conta que esta matéria está intrinsecamente ligada com os direitos fundamentais que gozam de proteção constitucional, logo, o tema em si representa o topo das nossas preocupações, pois devemos sempre nos lembrar a importância que a carta magna tem para questões do género.

---

[568] Paulo Alexandre Dias da Silva Constantino Teles, Natural de Luanda - Angola, Mestrando em Direito Judiciário na Universidade Europeia, frequentou uma pós graduação em Direito Penal Economico no IDPEE, da Faculdade de Direito da Universidade de Coimbra, licenciado em Direito pela Universidade Lusíadas de Angola,

Especializado em gestão de Informação pela GICHD/ CIDHG (Geneva Internacional Centre for Humanitarian Deminig/ Centro Internacional de Desminagem Humanitaria de Genebra). Funcionário Público em Angola, sendo actualmente o responsável pela área jurídica da Agência Nacional de Ação contra Minas.

Palavras-chave:

Proteção de dados, Direitos, Princípios, Constituição, Leis.

Proteção de dados ontem, hoje e amanhã

Abstract

This report deals with data protection over a period of time, that is, from the beginning to possible future challenges. Our objective is to better understand how data protection emerged, its purpose, the impact it has on our lives and to look from a deductive perspective at possible problems that may arise in the future. We understand that this issue has a unique relevance for the study of Law, because apparently, we are talking about a new branch of law, but in reality, it is not and its evolution has been as fast as the speed of light. In this context, this research was carried out based on a global reality, although the starting point was the European Union and also because we believe that this topic is a current and permanent issue, as we can see trough it´s development, growth and human dependence on new technologies. Furthermore, we also take into account that this matter is intrinsically linked with the fundamental rights that enjoy constitutional protection, therefore, the topic itself represents the top of our concerns, as we must always remember the importance of the great charter in such matters.

Keywords: Protection Regulation, Rights, Principles, Constitution, Laws.

Introdução

Este trabalho foi desenvolvido a partir de uma compreensão de que a liberdade humana é um dos princípios fundamentais do Direito, tendo em conta que a norma jurídica regula a conduta e o comportamento dos cidadãos, logo, deve haver mecanismos legais que fortaleçam os direitos de toda a pessoa em todos os momentos das suas vidas.

Ao longo da história o homem, os seus problemas e os seus valores fundamentais tiveram sempre uma atenção especial tanto pelo próprio homem (indivíduo) como pela própria sociedade, tal atenção radica do princípio da dignidade da pessoa humana, dos seus direitos inalienáveis, insuscetível de avaliação pecuniária e até dos mais simples direitos adquiridos fruto da dinâmica da determinação dos direitos fundamentais como um todo. Neste contexto, devemos dar capital importância aos efeitos do não cumprimento destes princípios pois acabam por violar os direitos destes indivíduos e desrespeitar toda e qualquer norma que visa garantir os mesmos.

Nas circunstâncias acima referenciadas, a problemática levantada neste relatório é essencialmente sobre o direito a proteção de dados e os seus referidos efeitos no nosso cotidiano, assim para melhor podermos entender devemos antes de tudo partir pela a defesa da dignidade da pessoa, desde a proteção ao seu bom nome, o direito a honra, a imagem, a privacidade, entre muitos outros.

Esta problemática vem trazer a ribalta a defesa da exposição da vida privada do ser humano de um modo geral, pois, por força da evolução da tecnologia e a possível propagação dos dados pessoais para os mais variados fins, surge a necessidade de se estabelecer normas que consigam ater a violação da dignidade da pessoa humana. Logo, a nossa luta visa entender como e de que forma podemos encontrar soluções plausíveis para garantir que os nossos dados pessoais estejam bem salvaguardados diante da velocidade da evolução tecnológica e de modos a garantir a proteção de facto da exposição indevida do homem como tal.

Por último, este relatório é extremamente importante para mim, pois, como funcionário publico trabalhei com dados pessoais durante muito tempo, em suma, reconheço a relevância do tema.

1. Conceito

O professor Menezes Cordeiro entende que a proteção de dados é "o conjunto sistematizado de princípios, normas e institutos que regulam os dados pessoais e o seu tratamento,"[569] isto pelo menos numa perspetiva teórica, pois se olharmos para a questão de forma prática iremos entender que neste conceito, não encontramos denominadas as pessoas coletivas, logo, concordamos com professor Menezes Cordeiro quando diz que muito embora esta definição esteja correta, porém, a verdade é que esta definição esta desatualizada para os dias de hoje, em outras palavras não se adequa aos desafios e a própria realidade atual.

Todavia, também devemos aqui salientar que nos termos do nº. 1 do artigo 1º do RGPD[570] a definição que está correta é a primeira, logo, será que devemos considerar que a posição adotada por nós cai por terra? Não acredito, pois, a proteção de dados querendo ou não envolve as pessoas coletivas, mas esta questão vamos esgotar num outro momento.

2. A evolução do Direito de proteção de dados

É difícil situar o início do Direito europeu de proteção de dados. A verdade é que esta questão surge com a utilização de mecanismos automatizados no processamento de informação pessoal, é assim que na década de 60, os pioneiros desta referida década identificaram os riscos do tratamento automatizado de dados para a privacidade do homem comum e devemos aqui salientar que os riscos que foram apresentados nesta altura ainda hoje são de grosso modo a maior preocupação do RGPD, que é essencialmente o controlo e o tratamento dado as informações que partilhamos com as mais variadas entidades, sejam elas de carater público ou privado[571].

Contudo e de acordo as nossas pesquisas podemos considerar que o ano de 1970 pode ser tido como o ponto de partida, pois foi através dos trabalhos preparatórios do Hessisches Datenschutzgesetz que este termo foi empregue pela

---

[569] MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 35.

[570] Art. 1º, nº 1 – O presente regulamento estabelece as regras relativas a proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e a livre circulação; nº 2 – o Presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito a proteção de dados pessoais; nº 3 – A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

[571] MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 37.

primeira vez[572] e consequentemente, também nesta mesma data aprovada a primeira Lei de proteção de dados do mundo no estado de Hesse, na Alemanha[573]. Entretanto uma questão que não podemos deixar de dizer e que de certo modo devemos reter é que o Direito da Proteção de Dados nesta época surgiu através do Direito público, tendo em conta que o primeiro diploma sobre esta matéria apenas visava as entidades publicas como seus fies destinatários[574].

Tal como frisarmos anteriormente, o legislador ao estatuir regras vinculantes para a forma de lidar com dados pessoais, baseou-se nos conselhos provenientes dos pioneiros da década de 60, tal como podemos extrair das conclusões oriundas das audiências realizadas pelo congresso, em 1965, do "Special Subcommittee on Invasion of Privacy[575]" ou ainda nas audiências de 1966 em que Charles A. Reich apresentou as suas preocupações sobre a constituição do "National Data Center[576]" e por ultimo podemos citar outra audiência que foi a "the computer and invasion of privacy." Estas audiências foram tão importantes que acabaram por influenciar os legisladores americanos e europeus sobre esta referida matéria e deu origem ao "Fair credit Reporting act[577]". Este "act" teve essencialmente a função de proteger os consumidores individuais, pois, os legisladores americanos já entendiam que a proibição de tal prática afetaria o sector financeiro[578].

Outra data extremamente importante com o desenvolvimento do direito europeu de proteção de dados coube a uma decisão do Tribunal Constitucional Federal (TCF) alemão de 1983, que atribuiu pela primeira vez à proteção de dados uma dimensão relacionada ao direito constitucional e aos direitos humanos, tal ato fez com que esta proteção se fixasse como um pilar dentro da doutrina jurídica sobre a proteção de dados, facto que podemos notar na atual legislação europeia.

---

572 MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 31.

573 DÖHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia (Em linha), Revista Direito Público, 2020, volume 17, nº. 93, pág. 11, disponível: https://doi.org/10.11117/rdp.v17i93.4235

574 MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 39.

575 MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 53.

576 O'MARA, Margaret - The End of Privacy Began in the 1960s. (Em linha) - The New York Times, 5 de dezembro de 2018. Disponível em https://www.nytimes.com/2018/12/05/opinion/google-facebook-privacy.html

577 O "Fair Credit Reporting Act" foi criado com a intenção de controlar a atividade desenvolvida pelas agências de crédito.

578 MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 58.

O tribunal alemão fundamentou seu procedimento com base em factos verídicos, pois ao entregarmos os nossos dados apenas cabe a nós avaliar de que modo as nossas informações estão armazenadas e se podemos confiar na entidade que faz o referido tratamento dos nossos dados, pois a consequência do mau uso destes dados pode causar danos irreparáveis, em outras palavras ninguém melhor do que o proprietário dos dados para analisar a questão da forma que achar mais conveniente[579]. Outrossim, a decisão tomada pelo TCF de certo modo acabou por elevar a proteção de dados ao mesmo patamar dos direitos fundamentais pelo menos no que diz respeito a legislação europeia.

3. A Privacidade versus a Proteção de dados

Ao olharmos para o artigo 8º da Carta dos Direitos Fundamentais da União Europeia e conjugado com o nº. 2 do artigo 16º do Tratado sobre o funcionamento da União Europeia, podemos concluir que de facto o direito a proteção de dados foi elevado a um nível dos direitos fundamentais tal como acabamos de citar, todavia, esta questão já está prevista desta forma desde o tratado de Lisboa tal como conseguimos constatar através das nossas pesquisas. Todavia, ao olharmos para o artigo 7º da Carta dos Direitos Fundamentais da União Europeia vamos constatar que a mesma retrata a questão do respeito pela vida privada e familiar. Este direito que também é tido na esfera jurídica como um direito fundamental e por sinal também está consagrado na Constituição da República Portuguesa (CRP), mais concretamente no seu artigo 26º.

A importância deste artigo é tão grande que constatamos que o mesmo vem depois da proteção ao direito a vida prevista no artigo 24º e da proteção do direito a integridade pessoal previsto no artigo 25º ambos da CRP. De acordo a doutrina os direitos de personalidade previstos no artigo 26º da CRP fazem parte dos direitos fundamentais, de tal modo que estes acabam por impor limites a outros direitos fundamentais sempre que estes colidirem e devemos ainda ressaltar que estes mesmos direitos também gozam de proteção no âmbito do Direito Penal[580]. Assim ao lermos o artigo 26º é notório que o mesmo versa essencialmente sobre a identidade pessoal e podemos defini-la como aquilo que caracteriza cada pessoa enquanto unidade individualizada que se diferencia das demais pessoas por força da sua vivência pessoal[581].

---

[579] DÖHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia (Em linha), Revista Direito Público, 2020, volume 17, nº. 93, pág. 12, disponível: https://doi.org/10.11117/rdp.v17i93.4235

[580] MIRANDA, Jorge e MEDEIROS, Rui - Constituição Portuguesa Anotada, Coimbra, 2005, pág. 194.

[581] CANOTILHO, Gomes e MOREIRA, Vital - Constituição da República Portuguesa Anotada, Coimbra, 3ª ed. 1993, pág. 282 a 284.

É neste contexto que a jurisprudência italiana defende que a uma boa parte destes direitos fundamentais previstos no artigo 26º da CRP são na verdade a base para a determinação para a identidade pessoal e como consequência estes gozam de inúmeras proteções e não devem ser atropelados em algum momento tal como podemos extrair do nº. 1, do artigo 34º, do nº. 3, do artigo 35º, ambos da CRP.

Podemos também chamar o artigo 80º do Código Civil, pois, entende o professor Abílio Neto que a lesão da identidade pessoal, ou seja, da personalidade é, em princípio, ilícita, logo a dignidade das pessoas exige que lhes sejam reconhecidos um espaço para a sua privacidade, e esta privacidade deve se considerada como uma regra e nunca como exceção, em outras palavras, o direito a privacidade só pode ser legitimamente agredido quando um interesse publico superior o exija[582]. É dentro deste prisma que o professor Gomes Canotilho defende que o tratamento de dados pessoais deve processar-se no estreito respeito pela reserva da vida privada, pois de forma contrária estaríamos a obter e utilizar estas informações de forma abusiva por não termos o consentimento do proprietário dos dados em causa e que por sinal tais práticas atuam em oposição a dignidade da pessoa humana[583].

Diante desta realidade notamos que a jurisprudência do Tribunal Europeu de Justiça não têm feito uma distinção substancial entre os estes dois direitos fundamentais. Em decisões anteriores, aceita-se a concorrência ideal, mas, em decisões mais recentes, a relação entre ambos também é deixada em aberto. Todavia, acreditamos que isso não altera o facto de haver uma distinção entre estes dois princípios, ou seja, a privacidade pode ir além do direito à proteção de dados em sua exigência de proteção, e a proteção de dados também pode ir além da privacidade[584].

Em suma, a privacidade e a proteção de dados podem se fortalecer e complementar mutuamente, tendo em conta o papel fulcral que ambos detêm para a realização efetiva da proteção de dados.

---

[582] NETO, Abílio - Código Civil Anotado, Ediforum edições, 20º ed, 2018, pág. 74, pontos 14, I, V, VI e VII.

[583] CANOTILHO, Gomes e MOREIRA, Vital - Constituição da República Portuguesa Anotada, Coimbra Ed, 3ª

ed. 1993, pág. 294 e 295.

[584] DÖHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia (Em linha), Revista Direito Público, 2020, volume 17, nº. 93, pág. 14, disponível: https://doi.org/10.11117/rdp.v17i93.4235

4. Diretiva de Proteção de dados da União Europeia (95/46/CE)

A Diretiva de Proteção de dados da União Europeia (95/46/CE) foi a primeira grande legislação da Europa, ou seja, o grande marco em termos de legislação e evolução, pois, foi através desta diretiva que a Europa na pessoa da UE assumiu a posição pioneira na luta e na defesa da proteção de dados.

Neste contexto, é de extrema importância realçar que muito antes da consagração da proteção de dados como direito fundamental na Carta dos Direitos Fundamentais da União Europeia ou mesmo no Tratado sobre o funcionamento da União Europeia, foi promulgada essa, que entrou em vigor em 1995.

Todavia, a mesma teve enumeras dificuldades de tal modo que podemos extrair esta conclusão através da sua eficácia durante o seu tempo de vida útil. Contudo, um dos motivos para a existência desta realidade tem a ver com o fato de que os antigos tratados da Comunidade Europeia não tinham uma norma semelhante à do nº. 2, do artigo 16º, do TFUE e é por esta razão que esta questão anteriormente era resolvida através da chamada competência de mercado interno, prevista nos termos do artigo 94º[585] e do nº. 1 do artigo 95º[586], ambos do Tratado constitutivo da Comunidade Europeia.

5. O Regulamento Geral sobre a Proteção de Dados (2016/679/UE)

Existe toda uma necessidade de enaltecer a existência da Diretiva da Proteção de Dados, pois, esta diretiva já previa uma regulamentação abrangente dos tratamentos de dados pessoais de uma forma geral. Assim, a DPD já continha as estipulações essenciais em termos de conteúdo que também se encontram no RGPD e a título de exemplo podemos citar a necessidade de justificar um tratamento de dados mediante o consentimento ou um fundamento jurídico; a vinculação do tratamento de dados a diversos princípios; a vinculação à finalidade, a responsabilidade do agente de tratamento dos dados e a minimização de dados; a instituição de autoridades de fiscalização independentes, bem como a garantia da proteção de dados mediante diversos direitos da pessoa afetada.

---

[585] Artigo 94. - O Conselho, deliberando por unanimidade, sob proposta da Comissão, e após consulta do Parlamento Europeu e do Comité Económico e Social, adota diretivas para a aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros que tenham incidência directa no estabelecimento ou no funcionamento do mercado comum.

[586] Artigo 95º - n.º 1. Em derrogação do artigo 94º e salvo disposição em contrário do presente Tratado, aplicam-se as disposições seguintes à realização dos objectivo enunciados no artigo 14º. O Conselho, deliberando de acordo com o procedimento previsto no artigo 251º, e após consulta do Comité Económico e Social, adota as medidas relativas à aproximação das disposições legislativas, regulamentares e administrativas dos Estados- Membros, que tenham por objeto o estabelecimento e o funcionamento do mercado interno.

A verdade é que o RGPD é nos dias de hoje uma legislação extremamente importante pois, a cada dia que se passa notamos a evolução da vida humana por influência das novas tecnologias. Vejamos, antigamente, a intenção de contratar alguém dependia de uma entrevista presencial, mas nos dias de hoje, já é possível que estas entrevistas sejam realizadas de forma virtual.

Outro ponto não menos importante tem a ver com a velocidade e dinâmica introduzida pelos meios de tecnologia, se nos tempos mais remotos o envio de uma carta, telegrama, demorava dias ou meses, atualmente estamos a falar de frações de segundos, isto se olharmos para os emails. Assim, podemos também citar as compras online entre muitos outros pormenores, porem, a verdade é que na maior parte das nossas ações virtuais, deixamos o que os "hackers" chamam de "foot print" ou seja, a nossa pegada digital e esta pegada digital pode, e por norma demonstra ou revela, inúmeras informações sobre nós, não é à toa que nos anos sessenta (60) já os pioneiros desta questão levantaram esta preocupação, das informações estarem à disposição de qualquer pessoa.

Todos estes desafios aqui citados por nós é que foram a grande fundamentação para o surgimento deste regulamento. A "priore" podemos até olhar e confundirmos algumas áreas do direito, tais como o Direito do Consumidor, mas a verdade é que o Direito da proteção de dados, se tem na sua essência alguma interligação com o direito do consumidor, apenas pode ser para proteger o consumidor sempre que existir a possibilidade de exposição dos seus dados.

Outra área que também tem a sua razão de ser citada é a do Direito de Comércio Internacional, pois, para que existisse um equilíbrio foram criadas as normas ou os hábitos e costumes utilizados no Direito de Comercio Internacional, nomeadamente, a "Lex Mercatoria", como por exemplo, a feira de Burges. É assim que nesta mesma perspetiva, urge a necessidade de se criar normas que fossem tão abrangentes para de facto orientar esta questão.

Ao avaliarmos o impacto do RGPD e o da "Lex Mercatória" acredito que podemos assumir que elas acabam por realizar, de certo modo, o sonho dos doutrinadores de Direito Privado Internacional, ou seja, o sonho de existir uma legislação supranacional. A EU, ao dar este passo que, com toda a certeza, acabou por impactar a todos nós, também ditou as regras do mercado, pois esta norma, que tem sido a base dos demais países, não só pela forma como ela foi concebida, mas também pelas questões que ela impõe dentro do próprio regulamento.

Vejamos, nos termos do artigo 2º, que versa sobe o âmbito de aplicação material e do artigo 3º, que versa sobre o âmbito de aplicação territorial, vamos notar que o nº 1, do artigo 2º determina que a aplicação deste regulamento se dá apenas ao tratamento de dados pessoais, sendo estes automatizados ou não, logo, para entendermos melhor este artigo temos de recorrer a previsão do artigo 4º, que chama para a sua responsabilidade a definição dos conceitos deste regulamento,

assim, encontramos no nº. 1 deste artigo a definição de dados pessoais que é entendida como "toda informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular," e o nº. 2 versa sobre a definição de tratamento, que consiste em "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição."

Após a analise destes dois conceitos passamos então para a interpretação do artigo 3º, mais concretamente dos nºs. 1[587] e 3[588] do mesmo artigo, vamos poder concluir a ideia de que já vínhamos a defender, sobre a possibilidade de se ter uma norma cujo alcance é supranacional, logo e de acordo a previsão deste artigo a proteção dos dados ultrapassa as fronteiras da UE, visto que todas as ações realizadas dentro da UE gozam de proteção, tal como todas aquelas que vão para além das fronteiras, mas que sejam realizadas por cidadão ou entidade da EU, também goza desta mesma proteção.

O professor Menezes Cordeiro vai mais distante e assume que a expressão cidadão da UE, vai muito além do que esta previsto nos termos do artigo 9º[589] do TUE, pois entende o nosso excelentíssimo professor que este conceito no RGPD é tão abrangente que engloba os residentes permanentes ou temporários, turistas, trabalhadores temporários, apátridas e quaisquer outros sujeitos[590].

---

[587] O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

[588] O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

[589] Em todas as suas atividades, a União respeita o princípio da igualdade dos seus cidadãos, que beneficiam de igual atenção por parte das suas instituições, órgãos e organismos. É cidadão da União qualquer pessoa que tenha a nacionalidade de um Estado-Membro. A cidadania da União acresce à cidadania nacional e não a substitui.

[590] MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 74.

No nº. 11, do artigo 4º, vamos encontrar a definição do consentimento, este conceito é extremamente importante para nós, tendo em conta que o mesmo, ao nosso ver, deve assumir a posição de um princípio estruturante do RGPD, pois, de acordo o próprio regulamento, os princípios estão previstos no capítulo II e o consentimento não é um deles, todavia, reiteramos que o consentimento deveria, sem sombra de dúvidas, ser um princípio. Defendemos esta posição pois acreditamos que sem o consentimento do proprietário dos dados pessoais, seria praticamente impossível falarmos sobre o direito dos dados pessoais, tal como, conseguimos notar em passagens anteriores do nosso relatório, a proteção de dados visa no final de tudo proteger a dignidade da pessoa humana, como seria isso possível sem o consentimento?

Neste contexto o RGPD define o consentimento como "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento."

Logo, encontramos maior reforço para esta questão nos termos do nº. 1, do artigo 7º, do RGPD. O nº. 1 deste artigo é explicito, mas podemos interpretá-lo de forma extensiva pois, de acordo as nossas pesquisas, concluímos que não basta que o responsável pelo tratamento obtenha o consentimento do titular dos dados, mas exige-se-lhe que demonstre que o consentimento foi efetivamente assentido.

Outrossim, do responsável pelo tratamento espera- se, igualmente, que demonstre o cumprimento de todas as exigências formais e substantivas das quais depende um válido e legítimo consentimento. Trata-se de uma manifestação do princípio da realidade tal como reza o nº. 2, do artigo 5º, também do RGPD[591].

O capítulo III retrata toda a matéria relevante aos direitos do titular dos dados, assim, neste capítulo vamos encontrar apenas onze artigos, mas vamos apenas analisar três destes artigos e começaremos pelo artigo 12º, basicamente o referido artigo estabelece as regras que têm como objetivo complementar os direitos dos titulares dos dados, presentes nos artigos 13º a 22º e 34º. Em termos mais concretos, o artigo 12º trata de duas questões essencialmente:

(I) da transparência quanto as informações e comunicações do responsável perante o titular, incluindo regras de como as informações e comunicações devem ser prestadas; e

(II) procedimentos legais e técnicos quanto ao exercício dos direitos do titular, que vinculam tanto o responsável, quanto o titular. Esta disposição esta em total harmonia com o art. 8º da CDFUE, que corresponde ao princípio da soberania sobre

[591] MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 121.

os dados (Datenhoheit) do titular só poderá ser materialmente alcançado mediante informação compreensível, em todas as fases de tratamento[592].

O art. 13º[593] por sua vez versa sobre a informação e o acesso aos dados pessoais, todavia, é do nosso entender que se conjugarmos este artigo como o 15º,

[592] MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 148 a 149.

[593] 1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta- lhe, aquando da recolha desses dados pessoais, as seguintes informações:

a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;

b) Os contactos do encarregado da proteção de dados, se for caso disso;

c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;

e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

2. Para além das informações referidas no n.º 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:

a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;

b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

d) O direito de apresentar reclamação a uma autoridade de controlo;

e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;

f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente,

que visa garantir o Direito de acesso do titular aos seus dados vamos perceber que um esta intrinsecamente ligado ao outro, pois, o artigo 13º corresponde a todos os deveres que o responsável pelo tratamento dos dados tem de efetuar ou realizar no momento em que o titular dos dados o transmite os referidos dados, já o artigo 15º[594]

bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

3. Quando o responsável pelo tratamento pessoal tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.º 2.

4. Os n.ºs 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações.

[594] 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

a) As finalidades do tratamento dos dados;

b) As categorias dos dados pessoais em questão;

c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;

f) O direito de apresentar reclamação a uma autoridade de controlo;

g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.º relativo à transferência de dados.

3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.

4. O direito de obter uma cópia a que se refere o n.º 3 não prejudica os direitos e as liberdades de terceiros.

corresponde ao poder de execução que o titular dos dados tem para garantir que os seus dados estão bem protegidos e dentro do prisma em que lhe foi transmitido a data da celebração do referido contracto ou mesmo da transmissão dos referidos dados pessoais. Este poder concedido ao titular dos dados está também previsto na carta magna, mais concretamente no nº. 1, do artigo 35º[595] e, se analisarmos bem este artigo da CRP, vamos concluir que ele dá cobertura total ao artigo 15º do RGPD[596].

Outro artigo não menos importante é o 23º, que tem como finalidade tratar das limitações que podem ser impostas na eventualidade de se por em risco aspetos fundamentais da vida social do próprio Estado. Por norma, partimos da presunção que o direito a proteção de dados é absoluto, mas ao analisarmos o nº 1, deste artigo, chegamos a uma conclusão relativamente diferente que consiste no facto deste direito não ter um caracter absoluto e inclusivamente, acreditamos que foi por esta razão que a UE decidiu criar este artigo, tendo em conta que o mesmo já estava previsto na Diretiva 95/46, mais concretamente no seu artigo 13º, contudo, o seu alcance era relativamente menor.

É de capital importância termos em conta que os aspetos delimitados neste artigo que dão a possibilidade se violar o direito a proteção de dados, apenas pode ser executado através de uma medida legislativa, mas, esta medida deve sempre ter um caracter proporcional e acima de tudo deve sempre primar pelo respeito dos direitos e liberdades fundamentais do proprietário dos dados. Em suma este artigo delimita o alcance da própria norma, determinando em que momentos e de que forma os responsáveis ou os subcontratantes da proteção de dados têm o dever de trabalhar com o Estado de modos a proteger o nosso "modus vivendi".

O capítulo IV do RGPD trata da responsabilidade do tratamento dos dados pessoais pelo contratante ou ainda pelo subcontratante. Este artigo remete-nos para uma das primeiras questões levantadas no presente relatório, que tem a ver com o conceito do Direito de proteção de dados, tendo em conta que no conceito estabelecido apenas fala sobre as pessoas singulares e não sobre as pessoas coletivas. É por esta razão que concordamos com o Professor Menezes Cordeiro quando o mesmo diz que o conceito está desatualizado.

Após uma análise chamou-nos atenção os artigos 33º e 34º, ambos do RGPD, que versam sobre a notificação às autoridades de controlo (33º) e aos titulares dos dados pessoais (34º), sempre que existir uma violação. Estes artigos chamaram a nossa atenção pelo simples facto de notarmos que ambos reforçam os princípios

[595] Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

[596] MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022, p. 175.

previstos nos termos do artigo 5º, com especial ênfase ao princípio da transparência e da lealdade. Outro artigo que também contribui bastante para este ponto que acabamos de frisar é o artigo 40º, que retrata o código de conduta que cuja finalidade é contribuir para a correta aplicação do RGPD.

Outro artigo que é extremamente importante para nós, é o 42º, que a nosso entender ajuda na decisão do titular dos dados sempre que este contratar ou transmitir os seus dados a uma determinada entidade, sabendo que se eles possuírem o referido selo, acabam por garantir que são entidades idóneas. Outrossim, este aspeto não se aplica só ao titular dos dados, mas também as entidades que são contratadas pela primeira vez quando estas decidem subcontratar um terceiro, logo, se este terceiro tiver o selo o contratante primário também fica assegurado que esta entidade subcontratada também é idónea.

Em suma estes artigos que acabamos de citar reforçam os princípios supracitados e acabam por garantir ao proprietário dos dados que estes (dados) estão bem salvaguardados e dentro de um ambiente que demonstra que existe efetivamente bastante transparência e lealdade.

O capítulo VI tem como finalidade abordar sobre as autoridades de controlo, pelos artigos 51º (autoridade de controlo), 52º (independência das autoridades de controle), 55º (competências), 57º (atribuições) e 58º (poderes). Contudo temos um pormenor que notamos, que para nós representa um ponto extremamente importante, pois o artigo 63º, que pertence ao capitulo XVII, cuja epigrafe é cooperação e coerência, representa para nós um momento muito importante, pois para salvaguardar a coerência e ao mesmo tempo garantir que as autoridades de controlo não tivessem poderes excessivos vem este artigo determinar os procedimentos que as autoridades de controlo devem seguir para garantir que todo e qualquer processo seja coerente.

O artigo 64º, mais concretamente no seu nº. 1, determina que cabe ao comité emitir um parecer sempre que a autoridade de controlo competente tenha a intenção de aplicar alguma medida, este artigo vai nos remeter para o artigo 68º e seguintes, que versam sobre o comité europeu para a proteção de dados. Em poucas palavras entendemos que o comité europeu é a autoridade que controla a aplicação normativa do RGPD, mas o faz em conjunto com as autoridades de cada Estado membro da UE.

Podemos ainda citar mais dois artigos que também demonstram ser relevantes, nomeadamente o artigo 88º, que visa regulamentar o tratamento dos dados pessoais no contrato laboral e o artigo 90º, cuja finalidade é impor a obrigação do dever de sigilo.

O RGPD é nada mais, nada menos, do que um diploma legal que visa orientar os demais Estados membros da UE, pois é sabido que posteriormente cada Estado tem o dever de criar uma norma interna sobre a proteção de dados para orientar

todas estas questões que acabamos de ver, assim, Portugal tem dois diplomas legais que tratam desta questão, nomeadamente a Lei nº. 58/2019 e a lei 59/2019. A primeira trata das questões ligadas as pessoas singulares enquanto a segunda trata das regras relativas ao tratamento de dados pessoais para efeitos de prevenção, detenção, investigação ou repressão de infrações penais ou de execução de sanções penais.

6. O amanhã da Lei de Proteção de dados

Falarmos sobre o amanhã da proteção de dados é uma questão extremamente complexa, desde já, existem questões que os anciões desta matéria apresentaram nos anos 60, que nos dias de hoje ainda nos deparamos com elas, tal como podemos constatar no livro de Vance Parckard, denominado "the naked society[597]", que critica o facto de os dados pessoais serem usados para esquemas comerciais, ou seja, de "marketing", e esta questão continua pertinente até os dias de hoje e notamos isso quando olhamos para um determinado número de fundos de investimentos, vamos notar que estes são detentores das maiores empresas a nível global e a título de exemplo passamos a citar algumas empresas que pertencem a estes fundos:

Amazon

Coca-Cola

Twitter

PepsiCo

Microsoft

Time Warner

Ferrari

Apple

Bank of America

JP Morgan

Wells Fargo

Citigroup

Monsanto

Goldman Sachs

[597] A sociedade nua.

Exxon Mobil

Johnson & Johnson

Ford

Pfizer

Mc Donald's

Uber

The Walt Disney Company

Estas empresas que acabamos de citar são apenas algumas das quais estes fundos de investimento são proprietários, logo, surge uma questão que não pode de alguma forma não ser feita, como é que falamos na proteção de dados quando temos entidades privadas com tanta influência a nível internacional, pois, se analisarmos bem vamos dar conta que estas entidades dominam o mercado financeiro em quase todos os sectores, começando pela industria farmacêutica, robótica, tecnológica, automóvel entre muitas outras.

Após esta pequena descoberta temos de analisar quanta informação em termos de dados estas empresas realmente detêm, pois, se nos dias de hoje para se fazer seja o que for precisamos de internet, logo, podemos aqui assumir que uma das principais páginas de buscas a nível global é a google, automaticamente sempre que realizamos uma pesquisa, acabamos por deixar exposto o nosso "footprint[598]", dito isso, as demais empresas podem aproveitar-se desta pequena informação que (para muitos especialmente os leigos na matéria) parece irrelevante e aproveita a oportunidade para direcionar a um grupo bem identificado uma proposta sobre um determinado produto e assim vai ser consecutivamente para as outras áreas.

Esta questão poderia ser vista como a questão dos monopólios, que numa determinada época os estudiosos das ciências económicas concluíram que os monopólios eram uma má influência para o crescimento das economias, logo, de forma análoga, recorro a esta mesma ideia e acredito piamente que esta é uma questão que pode afetar o verdadeiro crescimento da proteção de dados.

Vejamos, após a analise do RGPD, notamos que trata dos mais variados pontos, mas não impõe um determinado limite na forma como os dados são de facto utilizados, pelo quanto a sua finalidade, em outras palavras, antes de entrar em contato com esta matéria sempre pensei que quando desse os meus dados estaria simplesmente a inscrever-me num determinado "site", ou ainda a solicitar que a loja "x" enviasse-me informações sobre a sua próxima coleção, mas a verdade, é que os

[598] Footprint – é um termo oriundo do inglês cujo significado é pegada digital e isto significa ou visa identificar tudo que nos fizemos enquanto estamos a utilizar a internet.

nossos dados são muito mais do que isso e têm um valor muito maior do que nós imaginamos, pois, se quando realizamos uma pesquisa na internet seja, no Youtube, google entre muitos outros, vamos notar que posteriormente esta informação fica de certo modo predefinida, como a nossa busca ou procura primária, sempre que pesquisarmos outros sites online, logo de alguma forma os nossos dados são passados, inclusive até os nossos interesses acabam sendo estudados. Neste quesito, urge a necessidade de se criar balizas ou barreiras que venham de facto limitar ou direcionar como alguma imposição esta nossa preocupação.

Ao terminar esta análise surgiu-nos uma questão que não se quer calar e esta consiste em saber como empresas de carater social, como a Meta, por exemplo, que é a detentora do Facebook, Instagram e do WhatsApp, consegue ser ou estar na lista das empresas mais rentáveis do mundo, se ao nosso entender ela apenas serve para interação social? De que forma é que eles utilizam os nossos dados ou experiências socias? Apenas fizemos estas perguntas mas, poderíamos fazer muitas mais, pois ao nosso ver estas questões podem e devem ser levantadas para que num futuro próximo possamos definir de facto a verdadeira intervenção da proteção de dados e não ficarmos na incerteza se os nossos dados estão salvaguardados apenas para um determinado fim e no final descobrirmos que os nossos dados são utilizados para esquemas comerciais para enriquecerem outras pessoas sem o nosso conhecimento ou consentimento propriamente dito.

Outro aspeto não muito distante deste é o da evolução da própria ciência, por hoje temos questões que de certo modo estão interligadas, como é o caso dos meta-dados, dos cookies, da inteligência artificial entre muitos outros avanços. A forma como a ciência tecnológica evolui também é uma questão que apresenta os seus desafios para a o Direito, pois a forma como uma ciência evolui é totalmente diferente da outra, enquanto uma depende de descobertas e cérebros brilhantes a outra tem que necessariamente esperar por consensos sociais, pois, não podemos falar em direito "X" ou "Y" se não existirem normas que versam sobre o referido assunto, em outras palavras existem inúmeros protocolos para a criação ou alteração de uma norma e só isso acaba por retardar o efeito das normas jurídicas na vida social.

A título de exemplo podemos citar a própria lei de proteção de dados que como já vimos, já vem a ser debatida e retratada em vários diplomas e felizmente conseguiu alcançar o seu apogeu agora, com o surgimento do RGPD; outro exemplo é a chamada Diretiva ePrivacy nº 2002/58/CE ou a Diretiva Complementar nº 2009/136/CE, cuja finalidade é orientar a forma como se empregam os cookies para a área da telecomunicação. Estas normas continham alguns aspetos especiais ou mais específicos em comparação ao RGPD, também é bem verdade o RGPD trata da questão da proteção de dados num aspeto global enquanto estas duas normas em especial tratam essencialmente das proteção de dados dentro do âmbito das

telecomunicações, logo, é evidente que vamos encontrar alguns aspetos mais especificas e entre eles podemos citar por exemplo, os elementos constitutivos de permissão e regras de tratamento para dados de tráfego e de localização, as medidas de segurança técnico-organizacionais das operadoras e obrigações de fornecer informações, entre muitos outros pontos.

Um outro exemplo tem a ver com a inteligência artificial que até a presente data ainda não existe nenhuma norma ou regulamento concreto sobre esta matéria, apenas, podemos realçar que no final do ano de 2023 a UE chegou a um acordo provisório sobre a proposta de regras harmonizadas em matéria de inteligência artificial, o que ao nosso ver é excelente, mas a verdade é que estamos a falar de uma realidade que já vem sido desenvolvida desde a década de 1950 mas a sua primeira regulação na UE apenas esta a ser feita agora.

É dentro deste prisma que temos de analisar esta questão a velocidade do mundo tecnológico não é a mesma que a do mundo jurídico e este é apenas um aspeto, podemos ainda acrescentar que por norma um jurista não domina estas matérias de caracter tecnológico, pois esta tarefa recai ou cabe aos engenheiros informáticos, o que por sinal também já causa alguma dificuldade na altura de se fazer as normas e para que não bastasse, por regra os legisladores não têm todos os mesmo conhecimento e em muitos casos estes decidem consoante a sua experiencia de vida ou pareceres técnicos que os mesmos têm acesso, logo tudo isso, retarda a produção de normas eficazes e pontuais.

Em suma, uma questão que de facto devemos realçar é a forma como o direito a proteção de dados deverá evoluir, pois, a nosso ver o verdadeiro segredo esta nesta questão, a tecnologia, o comercio, entre outras atividades evoluem muito mais rápido que a ciência jurídica, logo, a luta deve ser tentar ser o mais assertivo no que tange a feitura das normas e tentar arranjar formas de se atualizar as normas o mais rápido possível, contudo, o futuro é uma questão incerta mas, podemos e talvez devemos tentar antever determinadas situações com o intuito de podermos futuramente colmatar determinados litígios que possam surgir.

Conclusão

No presente relatório tivemos a oportunidade de ver a questão da proteção de dados desde o primeiro momento e terminamos com uma perspetiva futurística, lembrando que as nossas posições tanto podem estar certas como não, isto de facto será um critério que devera ficar a cargo da ciência.

Começamos por abordar todas as questões relevantes para o nosso tema, desde o conceito de proteção de dados, a evolução, a distinção entre privacidade e proteção de dados, posteriormente falamos dos diplomais legais anteriores ao RGPD e consequentemente fizemos uma analise daqueles que consideramos ser os artigos mais relevantes do RGPD e por último analisamos alguns aspetos que ao nosso

ver podem e devem ser tidos em conta para puder garantir maior longevidade e eficácia na aplicação da própria regulamentação.

Durante a nossa exposição apresentamos várias questões que merecem alguma atenção, entre elas realçamos o facto de o conceito de proteção de dados apenas falar sobre as pessoas singulares e nunca das pessoas coletivas quando estas também devem fazer parte deste conceito, pelo menos no nosso entender, outrossim, é o facto de existirem empresas tao influentes que podem de algum modo criar algumas dificuldades na verdadeira aplicação das normas sobre a proteção de dados.

A grande conclusão que chegamos com este relatório é que ainda existem muitas questões para serem resolvidas, o nosso relatório focou-se apenas no continente europeu e não analisamos questões que vão para alem desta realidade, neste contexto, acreditamos que mesmo dentro da UE ainda há muito para se fazer, tal como também constatamos no próprio relatório que ainda existem outras normas que de certo modo estão interligadas com o RGPD, mas de uma forma mais especializada que estão a ganhar corpo para melhor responderem aos anseios de toda uma sociedade que visa ser protegida da melhor forma possível.

Em suma notamos que a problemática levantada por nós não se esgota aqui e ainda teremos de encontrar enumeras soluções, tendo em conta que no âmbito da arena internacional esta temática será sempre atual, pois, entendemos que as políticas e as normas que tratam da proteção de dados e as suas referidas soluções estão em constantes mudanças por força da dinâmica social e tecnológica, logo, podem surgir outras soluções ou problemas não abordados por nós.

Referências

CANOTILHO, Gomes e MOREIRA, Vital - Constituição da República Portuguesa Anotada, Coimbra Ed, 3ª ed. 1993.

DÖHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia (Em linha), Revista Direito Público, 2020, volume 17, nº. 93, pág. 14, disponível: https://doi.org/10.11117/rdp.v17i93.4235

MENEZES CORDEIRO. Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2022.

MIRANDA, Jorge e MEDEIROS, Rui - Constituição Portuguesa Anotada, Coimbra, 2005.

NETO, Abílio - Código Civil Anotado, Ediforum edições, 20º ed, 2018, pág. 74, pontos 14, I, V, VI e VII.

O'MARA, Margaret - The End of Privacy Began in the 1960s. (Em linha) - The New York Times, 5 de dezembro de 2018. Disponível em https://www.nytimes.com/2018/12/05/opinion/google-facebook-privacy.html

Legislação

DIÁRIO DA REPÚBLICA. Decreto de 10 de Abril de 1976 - Constituição da República Portuguesa, Diário de República n.º 86/1976, Série I de 1976-04-10, páginas 738 – 775, Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-aprovacao-constituicao/1976-502635

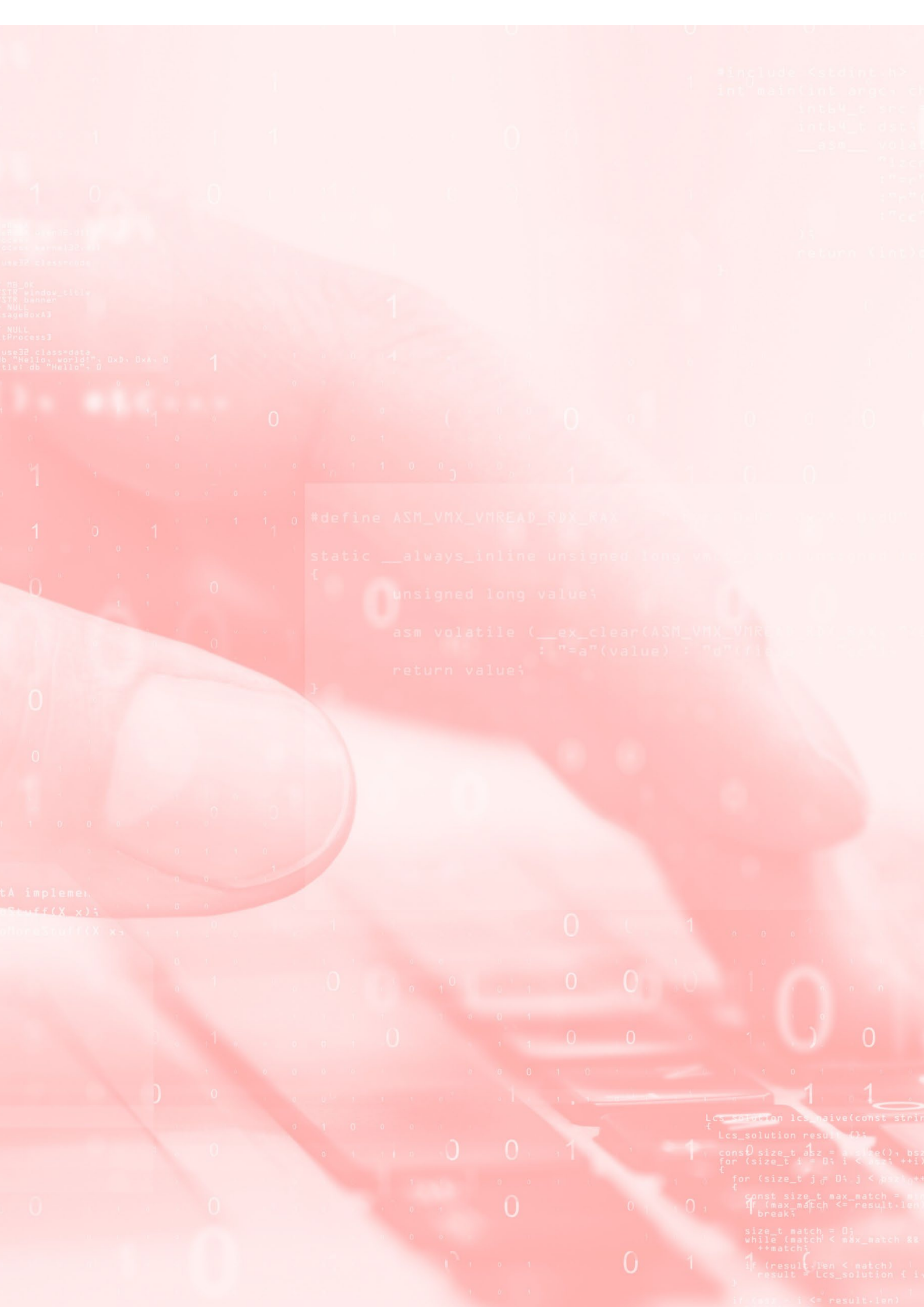
DIÁRIO DA REPÚBLICA. Decreto Lei n.º 47344/66, de 25 de Novembro - CÓDIGO CIVIL, Diário do Governo n.º 274/1966, Série I de 1966-11-25, páginas 1883 – 2086, Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/47344-1966-477358

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01). Jornal Oficial das Comunidades Europeias, 12 de dezembro de 2000. Disponível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial das Comunidades Europeias, L 281, 23 de novembro de 1995, Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=OJ:L:1995:281:TOC

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, 04 de maio de 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. Tratado sobre o Funcionamento da União Europeia (versão consolidada) Jornal Oficial das Comunidades Europeias, 07 de junho de 2016. Disponível em Tratado sobre o Funcionamento da União Europeia (versão consolidada) (europa.eu)



III
Legislação e Jurisprudência Comentadas

Privacy and Data Protection Magazine - Revista Científica na Área Jurídica
n.º 07-2024, abril 2024. ISSN: 2184-920X

Tribunal de Justiça da União Europeia

Caso Endemol Shine Finland

(Acórdão 7 março 2024, C-740/22, ECLI:EU:C:2024:216)

Acórdão do Tribunal de Justiça (Sexta Secção) de 7 de março de 2024. Pedido de decisão prejudicial apresentada por Itä-Suomen hovioikeus. Reenvio prejudicial — Proteção de dados pessoais — Regulamento (UE) 2016/679 — Artigos 2.o, 4.o, 6.o, 10.o e 86.o — Dados detidos por um tribunal relativos às condenações penais de uma pessoa singular — Comunicação verbal desses dados a uma sociedade comercial devido a um concurso organizado por esta — Conceito de "tratamento de dados pessoais" — Legislação nacional que regula o acesso aos referidos dados — Conciliação entre o direito do público de acesso a documentos oficiais e a proteção de dados pessoais. Processo C-740/22.

"[…] a comunicação oral de informações relativas a eventuais condenações penais em curso ou já cumpridas de que uma pessoa singular foi objeto constitui um tratamento de dados pessoais […] quando essas informações estejam contidas ou se destinem a figurar num ficheiro." (parágrafo 39)

"[…] o seu artigo 6.°, n.° 1, alínea e), e o seu artigo 10.°, devem ser interpretadas no sentido de que se opõem a que dados relativos a condenações penais de uma pessoa singular que figuram num ficheiro mantido por um órgão jurisdicional possam ser comunicados oralmente a qualquer pessoa para efeitos de garantir o acesso do público a documentos oficiais, sem que a pessoa que requer a comunicação tenha de justificar um interesse específico em obter os referidos dados, e a circunstância de esta pessoa ser uma sociedade comercial ou um particular não tem impacto a este respeito." (parágrafo 58)

Link: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62022CJ0740

Caso Iab Europe

(Acórdão 7 de março 2024, C-604/22, ECLI:EU:C:2024:214)

Acórdão do Tribunal de Justiça (Quarta Secção) de 7 de março de 2024. IAB Europe contra Gegevensbeschermingsautoriteit. Pedido de decisão prejudicial apresentada por Hof van beroep te Brussel. Reenvio prejudicial — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais — Regulamento (UE) 2016/679 — Organização setorial normativa que propõe aos seus membros regras relativas ao tratamento do consentimento dos utilizadores — Artigo 4.o, ponto 1 — Conceito de "dados pessoais" — Cadeia de letras e de carateres que captam, de forma estruturada e legível por uma máquina, as preferências de um utilizador da Internet relativas ao consentimento desse utilizador quanto ao tratamento dos seus dados pessoais — Artigo 4.o, ponto 7 — Conceito de "responsável pelo tratamento" — Artigo 26.o, n.o 1 — Conceito de "responsáveis conjuntos pelo tratamento" — Organização que não tem, ela própria, acesso aos dados pessoais tratados pelos seus membros — Responsabilidade da organização que abrange os tratamentos posteriores de dados efetuados por terceiros. Processo C-604/22.

"[…] uma cadeia composta por uma combinação de letras e de carateres, como a TC String, que contém as preferências de um utilizador de Internet ou de uma aplicação relativas ao consentimento desse utilizador para o tratamento dos dados pessoais que lhe dizem respeito por fornecedores de sítios Internet ou de aplicações, bem como por intermediários desses dados e por plataformas publicitárias, constitui um dado pessoal […]." (parágrafo 51)

Link: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62022CJ0604

IV
Recensões

Cristina Marai de Gouveia Caldeira[599]

A obra coletiva "Privacidade e Proteção de Dados do Município de Lisboa" reune um conjunto de doutrinadores, professores e investigadores de reconhecido mérito, nos domínios da privacidade e proteção de dados. O resultado é uma obra de natureza teórico-prática, uma referência nos domínios da privacidade, proteção de dados, inteligência artificial e governação de dados, que nos ajudará a trilhar os desafios que o cumprimento das normas de proteção de dados nos coloca.

O artigo de abertura é da autoria de António Barreto Menezes Cordeiro, uma resenha histórica do Direito da Proteção de Dados, desde os anos 60 do século XX até à contemporaneidade, na qual são elencados os principais conceitos e princípios que dão corpo a este ramo jurídico, autónomo, específico e eclético. Numa perspetiva histórica, salienta que embora o nascimento do Direito da proteção de dados tenha ocorrido nas fronteiras do Direito público, esta hegemonia foi quebrada, sendo a legislação na área da proteção de dados, aplicada, quer ao tratamento de dados produzidos por sujeitos de Direito público, quer por sujeitos de Direito privado.

Alexandre L. Dias Pereira, reflete sobre a proteção de dados pessoais a partir do Regulamento Geral de Proteção de Dados (RGPD), na perspetiva do responsável pelo tratamento, realçando as suas novas obrigações e, em especial o papel central do responsável pelo tratamento no regime jurídico dos dados das pessoas humanas. Conclui pela especial relevância da proteção dos dados pessoais no contexto da

[599] Pós-Doutorada na área da Propriedade Intelectual, Universidade Nova de Lisboa. Doutorada em Direito na Especialidade em Ciências Jurídicas e Políticas pela Universidade Autónoma de Lisboa (UAL) e Programa Doutoral em Ciência Política na especialidade de políticas públicas, Universidade Católica Portuguesa. Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College. Curriculum vitae: Ciência ID: 711B-87B9-6826. ORCID ID: https://orcid.org/0000-0001-6925-1877.

sociedade da informação, da economia digital e do desenvolvimento da Inteligência Artificial.

A segurança no tratamento dos dados aplicada ao poder local foi defendida pelo Manuel David Masseno, responsabilidade que o RGPD imputa, quer ao responsável pelo tratamento, quer ao subcontratante, e que está diretamente relacionada com o cumprimento dos princípios da integridade e confidencialidade. O risco associado à utilização das novas tecnologias para os direitos e liberdades das pessoas singulares, constitui uma matéria central amplamente tratada, com níveis de risco diferenciados atendendo à natureza, âmbito, contexto e finalidades do tratamento dos dados, exigindo que o responsável pelo tratamento proceda, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. A severidade e probabilidade do risco chama à colação as medidas técnicas e organizativas de proteção dos dados pessoais, nomeadamente a pseudonomização e anonimização, que são aplicáveis pelo poder local.

Tendo em conta a crescente tendência de publicação de conteúdos nas redes sociais pela Administração Local, Jorge Gomes da Silva, Maria de Medeiros, Maria Helena Silva e Telma Vitória, procuram demonstrar as principais consequências da publicação de fotografias e vídeos nestas plataformas, fornecendo, ao mesmo tempo, a partilha de boas práticas que contribuem para a melhoria da conformidade com o RGPD.

Isabel Celeste M. Fonseca e o Investigador Joel A. Alves, analisam a Orientação de 1 de abril de 2023, da CNPD, sobre a publicação na Internet das atas de reuniões de órgãos colegiais autárquicos e as respetivas consequências práticas.

Francisco Rodrigues Rocha aborda a temática da conservação dos dados pessoais e a dificuldade da aplicação prática dos prazos de conservação, tendo em conta a sua determinação prévia e abstrata.

Duarte Rodrigues Nunes, alude às implicações do Acórdão do Tribunal Constitucional n.º 268/2022, que reformulou a Lei n.º 32/2008, de 17 de julho, e em concreto, a questão sobre a admissibilidade (ou não), da obtenção e valoração de metadados, conservados pelos respetivos operadores, bem como das provas obtidas através destes.

Pedro Rebelo Botelho Alfaro Velez apresenta-nos, no seu texto, as visões contemporâneas dos direitos fundamentais, procurando traçar um panorama das diversas culturas de direitos, bem como das contraculturas alternativas nas atuais democracias ocidentais, com destaque para o quadro europeu, ainda que abrangendo o cenário norte-americano.

A partir de fontes normativas europeias e nacionais, Alexandre Sousa Pinheiro aborda a governação e a reutilização de dados, bem como a proteção de dados pessoais. Baseando-se na estratégia de dados da União Europeia, analisa a evolução do mercado de dados europeu, dando nota dos serviços de intermediação de dados. Analisa também, a conciliação do RGPD com as diversas formas de extrair informação.

Por último, Cristina Maria de Gouveia Caldeira, sublinha os resultados promissores da aplicação das novas tecnologias, em especial da Inteligência Artificial, no setor da saúde. A temática da vulnerabilidade da pessoa humana, designadamente na doença, é não só abordada no plano legal, mas também no plano da bioética. Refere ainda, que as circunstâncias que ditam a sua fragilidade, permitem-lhe também o gozo de um regime reforçado de proteção no âmbito do Direito Europeu.

Obra disponível em: https://www.lisboa.pt/atualidade/publicacoes-periodicas?tx_ameosfilemanager%5Baction%5D=info&tx_ameosfilemanager%5Bcontroller%5D=Explorer%5CFile&tx_ameosfilemanager%5Bfile%5D=920042&cHash=b9bae95ae79d6a3e72af25762aef1340


Universidade
Europeia