Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 01 – 2021
ONLINE

Direção Executiva e Editorial
Cristina Maria de Gouveia Caldeira
Alexandre Sousa Pinheiro

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

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

Número
001

Ano de Publicação
2021

Afiliação
Privacy and Data Protection Centre – Universidade Europeia

Autores
Alexandre Sousa Pinheiro
Amaro Santos Figueiredo
Carlos A. M. Duarte
Cristina Maria de Gouveia Caldeira
Elizabeth Accioly
Gabrielle Bezerra Sales Sarlet
Ingo Wolfgang Sarlet
Isabel Farinha
João Massano
José Conde Rodrigues
José Roberto Goldim
Luciano Alves dos Santos
Mafalda G. Carvalho
Manuel David Masseno
Márcia Santana Fernandes
Maria Cláudia Cachapuz
Maria Luiza Kurban Jobim
Pedro Rebelo Botelho Alfaro Velez

Prefácio
Alexandre Sousa Pinheiro
Cristina Maria de Gouveia Caldeira

Direção Executiva e Editorial
Cristina Maria de Gouveia Caldeira

ISSN
2184-920X

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Índice

II – OUTROS ESTUDOS

III – LEGISLAÇÃO E JURISPRUDÊNCIA COMENTADAS

IV – RECENSÕES

Prefácio

O nascimento de um periódico é sempre um momento de realização e esperança.
Corresponde a um trabalho que lhe é prévio e visa projetar no futuro ideias originais e fundações novas.

A Revista *Privacy and Data protection Magazine* é um dos frutos do trabalho realizado no *Privacy and Data Protection Centre* da Universidade Europeia, criado em abril de 2020. Foi sempre convicção dos fundadores do Centro que este só se desenvolveria com uma aposta na investigação, no aprofundamento da doutrina, um trabalho contínuo e diferenciado.

Assim, na origem esteve a definição das matérias de maior expressão para a divulgação e aprofundamento científico. Escolheram-se matérias com fundações fortes e temas firmados na doutrina e dessa análise chegou-se à Proteção de Dados Pessoais e aos Direitos Fundamentais, à Propriedade Intelectual, ao Direito do Consumo, ao Direito da Saúde, ao Direito do Ambiente, ao Direito Europeu, ao Direito Digital e à Inteligência Artificial.

O Centro seguiu o seu caminho em tempos de pandemia através de webinários sobre temas ligados à sua área de desenvolvimento natural, apostando na excelência dos convidados e palestrantes e na regularidade das organizações.

A presente *Privacy and Data protection Magazine* insere-se na evolução natural do Centro, passando-se de um momento de divulgação do conhecimento para uma fase de participação formal no universo jurídico nacional, e aberto ao exterior, entrando no ecossistema das publicações científicas na area jurídica.

A internacionalização e a diplomacia científica foram sempre uma ambição do Centro, quer no espaço de lingua portuguesa, na língua espanhola, quer na fala do mundo globalizado.

Como sempre acontece no trabalho intelectual, entrega-se a obra nas mãos dos leitores, esperando que traga benefícios a quem estuda os temas nela versados. Haverá outros passos no futuro do Centro, mas o lançamento da Revista é um símbolo maior de maturidade de uma jovem unidade de conhecimento.

I_Artigos Doutrinários

O Direito Fundamental à Proteção de Dados Pessoais na Constituição Federal Brasileira de 1988[1]

Ingo Wolfgang Sarlet[2]

RESUMO

A Constituição Federal brasileira de 1988 não contempla no seu texto um direito fundamental autônomo à proteção de dados pessoais. A despeito disso, a doutrina jurídica e o Supremo Tribunal Federal brasileiro reconhecem tal direito como implicitamente protegido pela ordem constitucional. Nessa perspectiva o presente texto tem por objetivo apresentar e discutir alguns dos aspectos mais relevantes concernentes ao direito fundamental à proteção de dados pessoais, designadamente, a sua justificação, seu conteúdo, as posições jurídicas subjetivas associadas, os deveres de proteção conexos, sua eficácia horizontal, bem como o problema da legitimidade das intervenções restritivas por parte do Estado.

PALAVRAS-CHAVE

Proteção de dados pessoais; Direito Fundamental; Constituição Federal brasileira.

[1] O presente texto corresponde à versão, parcialmente ajustada e atualizada, publicada sob o título Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988, Direitos Fundamentais & Justiça | Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020.

[2] Professor Titular de Direito Constitucional e Coordenador do Programa de Pós-Graduação em Direito (Mestrado e Doutorado) e Professor do Programa de Pós-Graduação em Ciências Criminais, ambos da Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre. Desembargador aposentado do Tribunal de Justiça do Rio Grande do Sul. Advogado e parecerista.

The Fundamental Right to Personal Data Protection in the Brazilian Federal Constitution of 1988

ABSTRACT

The Brazilian Federal Constitution of 1988 does not contemplate in its text an autonomous fundamental right to the protection of personal data. In spite of this circumstance, legal literature and the Brazilian Federal Supreme Court recognize such a right as implicitly protected by the constitutional order. This paper aims to present and discuss some of the most important aspects related to the fundamental right to personal data protection, namely it's justification, content, associated legal subjective positions, related state duties, it's horizontal effect and the problem of the legitimacy of state interventions.

KEYWORDS

Personal data protection; Fundamental Right; Brazilian Federal Constitution.

Introdução

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 assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica, política, cultural contemporânea no Mundo, fenômeno comumente designado de "*Ubiquituous Computing*"[3].

Nesse contexto, a proteção de dados, ademais de sua exponencial relevância econômica, social e mesmo cultural, passou, já de há muito, a se transformar numa questão jurídica de grande proporção, marcada por uma crescente complexidade e multidimensionalidade, ademais de dizer respeito a todos os domínios do Direito, enquanto estrutura regulatória.

Outrossim, nada obstante o problema da proteção dos dados não se restrinja aos dados armazenados, processados e transmitidos na esfera da informática e por meios digitais, pois em princípio ela alcança a proteção de todo e qualquer dado pessoal independentemente do local (banco de dados) e do modo pelo qual é armazenado, cada vez mais os dados disponíveis são inseridos em bancos de dados informatizados. A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social[4].

A despeito de a instituição e subsequente ampliação em termos quantitativos e qualitativos da proteção jurídica de dados pessoais ter iniciado no limiar da Década de 1970, mediante regulação na esfera da legislação infraconstitucional específica da matéria, como foi o caso do estado de Hessen, de 1970, na Alemanha, aliás, a primeira legislação específica sobre o tema no Mundo (embora naquela quadra não projetada para o mundo digital e não tendo caráter nacional),[5] o reconhecimento de um direito humano e fundamental à proteção dos dados pessoais, contudo, teve de esperar ainda um tempo considerável para ser incorporado de modo abrangente à gramática jurídico-

[3] Cf., por todos, KÜHLING, Jürgen. Datenschutz und die Rolle des Rechts. *In*: STIFTUNG FÜR DATENSCHUTZ (Ed). *Die Zukunft der informationellen Selbstbestimmung*. Berlin: Erich Schmidt Verlag, 2016. p. 49.

[4] Cf. lembram: MIRANDA, Jorge; MEDEIROS, Rui. *Constituição Portuguesa Anotada*. 1. ed. Coimbra: Coimbra Editora, 2006. p. 379-380.

[5] Note-se que a primeira legislação federal (âmbito nacional) alemã foi editada em 1977, ainda assim, muito precoce.

constitucional, à exceção dos paradigmáticos exemplos da Constituição da República Portuguesa de 1976[6] e da Constituição Espanhola de 1978[7].

Nesse sentido, note-se que mesmo já no limiar da terceira Década do Século XXI, ainda existem Estados constitucionais onde um direito fundamental à proteção de dados não é reconhecido, pelo menos na condição de direito expressamente positivado na Constituição, muito embora tal direito seja, em vários casos, tido como implicitamente positivado, sem prejuízo de uma mais ou menos ampla regulação legislativa e administrativa, ademais de significativo desenvolvimento na esfera jurisprudencial.

No caso do Brasil, como se verá com maior detalhamento mais adiante, inexiste, por ora, previsão expressa de direito fundamental autônomo à proteção de dados pessoais na CF, nada obstante a tramitação, no Congresso Nacional, de uma proposta de emenda à constituição (PEC nº 17/2019), com tal objetivo.

À vista de tais considerações, a pergunta que se coloca e que se pretende responder ao longo do texto, é se é possível afirmar a existência de um direito fundamental à proteção de dados pessoais na ordem jurídica brasileira mesmo antes de vir a ser formalmente integrado ao texto constitucional, caso isso de fato venha a ocorrer e, em sendo positiva a resposta, qual o seu conteúdo, suas funções e seus limites.

Tal questionamento, por sua vez, assume ainda maior relevo com a edição da nova Lei Geral de Proteção de Dados Pessoais do Brasil – LGPDB (Lei n. 13.709/2018), que recentemente entrou em vigor, embora ainda não de modo integral[8] -, porquanto embora tal legislação não sirva de base e justificação constitucional direta para o reconhecimento de um direito fundamental à proteção de dados pessoais, o conteúdo e o alcance da regulação legal (infraconstitucional) carece de limitação a partir do marco normativo constitucional, ainda mais levando em conta o leque de direitos fundamentais e mesmo

[6]A proteção dos direitos fundamentais no campo da informática está detalhadamente prevista no artigo 35 da Constituição Portuguesa, aqui transcrito na sua versão inicial: "(utilização da informática) 1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos". Note-se que tal dispositivo foi alterado três vezes por leis de revisão constitucional de 1982, 1989 e 1997, tendo sido substancialmente atualizado e ampliado.

[7]Art. 18, nº 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Cuida-se aqui, na versão original de 1978, de uma proteção indireta dos dados pessoais, visto que não há menção expressa aos mesmos.

[8]A LGPD brasileira entrou em vigor, depois de tentativas de prorrogação, em 18 de setembro de 2020, mas a parte relativa às sanções tem sua entrada em vigor prevista para agosto de 2021, por ora, além de a Autoridade Nacional de Proteção de Dados (ANPD) instituída pela LGPD também estar ainda em fase de estruturação.

outros bens e interesses de estatura constitucional por ela protegidos, mas também limitados.

Para que um adequado enfrentamento das questões formuladas seja possível, inicia-se com a caracterização do direito à proteção de dados pessoais como fundamental, como tal implicitamente positivado na ordem jurídico-constitucional brasileira (2), passando a analisar o seu objeto - âmbito de proteção (3), sua dimensão subjetiva e objetiva (4), seus titulares e destinatários (5) e o problema dos seus limites e restrições (6), encerrando com algumas considerações finais (7).

1. O direito à proteção de dados pessoais como direito fundamental implícito na Constituição Federal de 1988

Como já adiantado, um direito humano e fundamental autônomo na esfera do direito constitucional positivo e do direito internacional dos direitos humanos ainda não é de longe onipresente nos textos de boa parte das constituições (em especial as mais antigas) e dos tratados internacionais de direitos humanos.

Ao nível do direito internacional público, tanto no âmbito do sistema universal de proteção da ONU, quanto na esfera do direito europeu, um direito à proteção de dados tem sido deduzido em especial do direito à privacidade, embora com este não se confunda. Nesse sentido, a orientação adotada pela Comissão da ONU para Direitos Humanos, interpretando o alcance do artigo 17 do Pacto Internacional de Direitos Civis e Políticos, assim como a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE), forte no artigo 8º da Convenção Europeia[9].

Foi somente na Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (1981)[10], comumente intitulada de Convenção de Estrasburgo, bem como, quase vinte anos mais tarde, no artigo 8 da Carta de Direitos Fundamentais da União Europeia (doravante CDFUE), do ano 2000[11] - que

[9] Cf., por todos, SCHIEDERMAIR, Stephanie. Einleitung. *In*: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GENANNT DÖHMANN, Indra (Coord.). *Datenschutzrecht*. Baden-Baden: Nomos, 2019. p. 201.

[10] CONSELHO DA EUROPA. *Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais*, de 28 de janeiro de 1981. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 15 nov. 2019.

[11] PARLAMENTO EUROPEU. *Carta de Direitos Fundamentais da União Europeia*, de 7 de dezembro de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 15 nov. 2019.

o direito à proteção de dados finalmente alçou a condição de direito fundamental de natureza autônoma, mas vinculando, como tal, apenas os estados integrantes da União Europeia, o que se deu apenas com a entrada em vigor do Tratado de Lisboa, em 2009[12].

No caso do Brasil, como já antecipado, a Constituição Federal de 1988 (CF), embora faça referência, no art. 5.º, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), não contempla expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular, sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira.

A proteção dos dados pessoais, por outro lado – para além da referência ao sigilo da comunicação de dados – também encontra salvaguarda parcial e indireta mediante a previsão da ação de *habeas data* (art. 5.º, LXXII, da CF), ação constitucional, com *status* de direito-garantia fundamental autônomo, que precisamente busca assegurar ao indivíduo o conhecimento e mesmo a possibilidade de buscar a retificação de dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, ao mesmo tempo em que se trata de uma garantia procedimental do exercício da autodeterminação informacional[13].

Com relação ao sigilo da comunicação de dados, contudo, há que ter cautela, razão pela qual se impõe o registro, com base na lição de Danilo Doneda, de que não se trata, neste caso, do direito à proteção de dados pessoais em si e nem de seu fundamento direto. Para melhor compreensão da assertiva, valemo-nos aqui da própria fala do autor:

> [Se,] por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua "comunicação", conforme art. 5, XII, que trata da inviolabilidade da comunicação de dados. Tal interpretação traz consigo o risco de sugerir uma grande permissividade em relação à utilização de informações pessoais. Nesse sentido, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais...O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade.... Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica... A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho... A decisão tem sido, desde então, constantemente mencionada como precedente em julgados nos

[12] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba, *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 15 nov. 2019.
[13] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. *Revista Direitos Fundamentais & Justiça*, a. 12, n. 39, p. 185-216, jul./dez. 2018.

> quais o STF identifica que a natureza fundamental da proteção aos dados está restrita ao momento de sua comunicação[14].

À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto da CF, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode (e mesmo deve!) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF – os direitos à privacidade e à intimidade[15], no sentido do que alguns também chamam de uma "intimidade informática"[16].

Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana[17], que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa[18].

À vista do exposto e como ponto de partida para os desenvolvimentos supervenientes, há, pois, como aderir ao entendimento – hoje consagrado na literatura jurídica brasileira – de que, mediante uma leitura harmônica e sistemática do texto constitucional, a CF consagrou um direito fundamental autônomo implicitamente

---

[14]DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 262

[15]Cf. por todos DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[16] Cf., por exemplo, entre nós, SAMPAIO, José Adércio Leite. A suprema inviolabilidade: a intimidade informática e o sigilo bancário. *In*: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coord.). *Direitos fundamentais no Supremo Tribunal Federal*: balanço e crítica, Rio de Janeiro: Lumen Juris, 2011. p. 531 e ss.

[17]Cf. por todos, MOTA PINTO, Paulo. *Direitos de Personalidade e Direitos Fundamentais*: Estudos, Coimbra: Gestlegal, 2018, em especial, p. 33 e ss.

[18] MOTA PINTO, Paulo. *Direitos de Personalidade e Direitos Fundamentais*: Estudos, op. cit., p. 642 e ss.

positivado à proteção de dados pessoais[19], o que veio a ser confirmado recentemente (maio de 2020) pelo Supremo Tribunal Federal, em histórico e paradigmático julgado.

Isso se deu em especial no julgamento da Medida Cautelar na ADI 6387, DF, Relatora Rosa Weber, onde se discute a constitucionalidade da Medida Provisória 954, de 17.04.20, da Presidência da República, que atribuiu às empresas de telecomunicações (fixas e móveis) o dever de disponibilizar os nomes completos, endereços e números de telefone dos usuários PN e PJ para o IBGE durante a pandemia do COVID 19 para efeitos de uso direto e exclusivo de produção de estatísticas oficiais mediante entrevistas domiciliares. No caso, a justificação de um direito fundamental à proteção de dados pessoais, na condição de direito autônomo implicitamente positivado, seguiu a linha geral protagonizada pela doutrina jurídica acima referida.

Além disso, é de sublinhar que apenas em 2020, o Supremo Tribunal Federal proferiu quatro decisões relevantes relativas à proteção de dados pessoais. Para além do caso do IBGE, o tema foi tratado na ADPF 695 (Caso Abin/Denatran), na ADI 656 (Cadastros de dependentes químicos) e na ADI 6.529 (Caso Sisbin). Nesse último caso, a Corte decidiu que os órgãos componentes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) quando for comprovado o interesse público da medida, afastando qualquer possibilidade desses dados atenderem a interesses pessoais ou privados

À vista disso, é de se acompanhar o entendimento de Carlos Alberto Molinaro e Gabrielle Bezerra S. Sarlet, de que a proteção de dados pessoais – e o reconhecimento de um direito fundamental correspondente -, de certo modo, "confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes"[20].

Ainda nesse contexto, embora ainda em fase de deliberação no Congresso Nacional, não há como deixar de destacar a proposta de inserção, tal como previsto na

[19] Cf., em especial, o já referido DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*, op. cit, 2006, mas também, na sequência, entre outros, LIMBERGER, Têmis. *O Direito à Intimidade na Era da Informática*. Porto Alegre: Livraria do Advogado, 2007; RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. *Direito, Estado Sociedade*, n. 36, jan/jun. 2010, MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor*. São Paulo: Saraiva, 2013, BIONI, Bruno Ricardo. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019. p. 90 e ss. Por último, v. SARLET, Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988, Direitos Fundamentais & Justiça | Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020.

[20] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. *Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data*. Direitos Fundamentais & Justiça, a. 13, n.41,p. 183-212, jul./dez. 2019.

PEC nº 17/2019[21], de um direito fundamental à proteção de dados pessoais no catálogo constitucional de direitos, mediante a inclusão de um inciso XII-A no artigo 5º, e o inciso XXX no artigo 22, estabelecendo, neste último caso, a competência privativa da União para legislar sobre a matéria.

Especificamente no concernente ao direito fundamental à proteção de dados, calha sublinhar que, a prevalecer a redação atual prevista no texto da PEC nº 17/19, aprovada na Câmara dos Deputados e que modificou a versão oriunda do Senado Federal, que acrescia um inciso XII-A ao artigo 5º sem alterar a redação original do inciso II, passará a ter o seguinte enunciado, inserindo o novo (?) direito no próprio texto do referido dispositivo:

> Art. 5º .....
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais; ..... (NR).

Outrossim, independentemente aqui de se aprofundar a discussão sobre a conveniência, necessidade e bondade intrínseca de uma consagração textual de um direito fundamental autônomo à proteção de dados na CF, ou mesmo adentrar a querela sobre se tratar, ou não, de um direito "novo", o fato é que cerramos aqui fileiras com os que saúdam como benfazeja tal medida.

Acrescente-se, outrossim, que, a teor do artigo 5º, §§ 2º e 3º, CF, o marco normativo que concretiza e formata o âmbito de proteção e as funções e dimensões do direito (fundamental) à proteção de dados, é também integrado – embora tal circunstância seja usualmente negligenciada – pelos tratados internacionais de direitos humanos ratificados pelo Brasil –, destacando-se, para o efeito da compreensão adequada e manejo correto em nível doméstico – a Convenção Americana de São José da Costa Rica e o Pacto Internacional de Direitos Civis e Políticos, incluindo a sua interpretação pelas instâncias judiciárias e não judiciárias respectivas.

Tal fato assume uma dimensão particularmente relevante, à vista do atual posicionamento do STF sobre o tema, dada a atribuição, aos tratados de direitos humanos devidamente ratificados, hierarquia normativa supra legal, de modo que, ao menos assim o deveria ser, o marco normativo nacional infraconstitucional não apenas deve guardar

[21] Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 15 nov. 2019.

consistência formal e material com a CF, mas também estar de acordo com os parâmetros de tais documentos internacionais, sendo passível do que se tem designado de um controle jurisdicional de convencionalidade. Além disso, convém lembrar que em se cuidando de tratados internacionais de direitos humanos aprovados pelo rito agravado previsto no § 3º do artigo 5º da CF o seu valor normativo na esfera nacional será equivalente ao das emendas constitucionais.

Nesse contexto, embora não exista (ainda) tratado internacional de direitos humanos específico sobre proteção de dados (ou mesmo tratado geral com referência direta e expressa a um direito humano correspondente) ratificado mediante tal procedimento, o fato é que tal circunstância não tem levado a um isolamento político-legislativo-jurídico do Brasil nessa matéria, do que dá conta, em caráter ilustrativo, a substancial recepção, pela nova LGPD, do Regulamento Geral Europeu, mas também, na esfera doutrinária e jurisprudencial, de parâmetros dogmáticos e interpretativos, como é o caso, já referido, de um direito à autodeterminação informativa, dentre tantos exemplos que poderiam ser colacionados.

Para encerrar essa primeira etapa do texto e dada a sua relevância não apenas para a compreensão do conteúdo e alcance do direito fundamental à proteção de dados na CF, mas também para efeitos de seu diálogo com a legislação, jurisprudência e mesmo doutrina sobre o tema, importa sublinhar que diversos diplomas legais em vigor já dispõe sobre aspectos relevantes da proteção de dados, destacando-se aqui a Lei de Acesso à Informação (Lei 12.527/2011) e o assim chamado Marco Civil da Internet (Lei 12.965/2014) e o respectivo Decreto que o regulamentou (Decreto 8.771/2016), mas especialmente a Lei Geral de Proteção de Dados (Lei 13.709, de 2018), que ainda se encontra na fase da *vacatio legis*, e que, salvo causa superveniente, deverá entrar em vigor, na sua plenitude, em 2021.

Assim, uma compreensão/interpretação/aplicação constitucionalmente adequada do direito fundamental à proteção de dados deverá sempre ser pautada por uma perspectiva sistemática, que, a despeito do caráter autônomo (sempre parcial), desse direito, não pode prescindir do diálogo e da interação (por vezes marcada por concorrências, tensões e colisões) com outros princípios e direitos fundamentais, que, dentre outros pontos a considerar, auxiliam a determinar o seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos.

Outrossim, o que é de particular relevância no caso brasileiro – justamente pela existência, além da nova LGPD, de outras leis que versam sobre o tema – é ter sempre

presente a necessidade de não apenas zelar pela consistência constitucional do marco normativo infraconstitucional no tocante aos diplomas legais isoladamente considerados, mas também de promover sua integração e harmonização produtiva, de modo a superar eventuais contradições e assegurar ao direito fundamental à proteção de dados, sua máxima eficácia e efetividade.

2. Âmbito de proteção do direito fundamental à proteção de dados pessoais

2.1. Para além da privacidade e da autodeterminação informativa

Como de certo modo já adiantado no segmento anterior, o conteúdo (no sentido do âmbito de proteção normativo) de um direito fundamental à proteção de dados pessoais, embora fortemente articulado com o princípio da dignidade da pessoa humana e de outros direitos fundamentais, em especial o direito ao livre desenvolvimento da personalidade e alguns direitos especiais de personalidade, como é o caso, entre outros, do direito à privacidade e do assim chamado direito à autodeterminação informativa, não se confunde com o do objeto da proteção de tais direitos.

É por tal razão, aliás, que a própria opção terminológica pela proteção de dados pessoais assume uma importância que vai muito além da mera novidade representada pela terminologia em si, porquanto, radica numa viragem concepcional, visto que parte do pressuposto de que dados, para efeitos de sua proteção jurídico-constitucional, devem ser compreendidos em sentido amplo, no sentido da inexistência de dados pessoais irrelevantes em face do processamento eletrônico na sociedade de informação, notadamente pelo fato de que, sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais[22].

De todo modo, a compreensão do âmbito de proteção de um direito fundamental à proteção de dados pessoais envolve sempre um contraste com o de outros direitos, destacando-se, nesse contexto, o direito à privacidade e o direito à autodeterminação informativa, os quais, por seu turno, embora também autônomos entre si, também apresentam zonas de contato importantes.

Pela sua relevância para o desenvolvimento do direito à proteção de dados pessoais, calha retomar, em rápidas pinceladas, o caso da Alemanha, porquanto é lá que

[22] Cf., por todos, MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): O Novo Paradigma da Proteção de Dados. *Revista de Direito do Consumidor*, v. 120, nov./dez. 2018. p. 22. Para maior desenvolvimento, v., em especial. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento, op. cit., p. 59 e ss.

se costuma situar o reconhecimento, pela primeira vez, do assim chamado direito à autodeterminação informativa, não no texto constitucional, mas por conta de paradigmática decisão do Tribunal Constitucional Federal, de 15.12.1983, sobre a constitucionalidade de aspectos da lei do censo aprovado pelo Parlamento Federal, cuja realização foi suspensa liminarmente pela Corte em 13.04.1983, muito embora a existência de decisões anteriores envolvendo, ao fim e ao cabo, a proteção de dados pessoais[23].

Na sua multicitada decisão, o Tribunal Constitucional Federal alemão, contudo, não reconheceu diretamente um direito fundamental à proteção de dados pessoais, mas sim, deduziu, numa leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, um direito fundamental implícito à autodeterminação informativa, que, consiste, em suma e de acordo com o Tribunal, na prerrogativa de cada indivíduo decidir em princípio e substancialmente sobre a divulgação e utilização de seus dados pessoais[24].

O próprio Tribunal Constitucional, contudo, na mesma decisão, alertou para o fato de que o direito à autodeterminação informativa não assegura a cada cidadão um controle absoluto sobre os seus dados, visto que, dada a inserção e responsabilidade comunitária e social do ser humano, este deve tolerar eventuais limitações do direito quando em prol do interesse geral[25].

De acordo com Hans-Peter Bull, primeiro encarregado da agência federal de proteção de dados alemã, o cerne moral e político das preocupações do Tribunal Constitucional foi (e é) o da garantia da liberdade dos cidadãos em face da repressão por parte do Estado, de modo que a argumentação deduzida na decisão foi orientada de acordo com o objetivo da proteção da liberdade de ação do ser humano, sendo a transparência da coleta de informações um meio para alcançar tal finalidade[26].

---

[23] Aqui costuma ser referida, dentre outras, decisão de 16.07.1969 ("Mikrozensus-Entscheidung"), na qual o Tribunal Constitucional assentou que a Lei Fundamental proíbe que o ser humano tenha sua inteira personalidade registrada e catalogada compulsoriamente (v. *BVerfGE* 27, p. 6).
[24] Cf., *BVerfG* 65, p. 42 e ss.
[25] Cf. *BVerfGE* 65, p. 44.
[26] Sobre a dedução interpretativa do direito pelo Tribunal Constitucional, v., por todos, a síntese de BULL, Hans-Peter. *Informationelle Selbstbestimmung* – Vision oder Illusion?. Tübingen: Mohr Siebeck, 2009. p. 29 e ss.

Na condição de direito de defesa (direito à não intervenção arbitrária) o direito à autodeterminação informativa consiste em um direito individual de decisão, cujo objeto (da decisão) são dados e informações relacionados a determinada pessoa-indivíduo[27].

A relação do direito à autodeterminação informativa com o princípio da dignidade da pessoa humana, portanto, é, em certo sentido, dúplice, pois se manifesta, tanto pela sua vinculação com a noção de autonomia, quanto com a do livre desenvolvimento da personalidade e de direitos especiais de personalidade conexos, de tal sorte que a proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta de tal desenvolvimento, para o qual a garantia de uma esfera privada e íntima são indispensáveis.

Não há sobreposição, contudo, entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar uma dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão dos seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*)[28].

Dito de outro modo, "a proteção de dados é, enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal"[29].

No concernente às suas interfaces com o direito à privacidade, também inexiste, como já adiantado, superposição completa dos respectivos âmbitos de proteção. Proteção de dados pessoais e, da mesma forma, autodeterminação informativa, vão além da privacidade e de sua proteção, ao menos no sentido tradicional do termo, caracterizado por uma lógica de "recolhimento" e "exposição"[30].

---

[27] Cf. ALBERS, Marion. Umgang mit personenbezogenen Informationen und Daten. *In*: HOFMANN-RIEM, Wolfgang; SCHMIDT-ASSMANN, Eberhard; VOSSKUHLE, Andrea (Coord.). *Grundlagen des Verwaltungsrechts*. 2. ed. München: C.H. Beck, 2012. v. 2. p. 146-47.

[28] Cf. HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The populational census decision and the right to informational self-determination. *Computer Law & Security Report*, v. 25, i. 1, 2009. p. 85-86.

[29] Cf. SPIECKER GENANNT DÖHMANN, Indra. Kontexte der Demokratie: Parteien, Medien und Sozialstrukturen (1. Referat). *VVDStRL*. Berlin: De Gruyter, 2018. v. 77. p. 55-56.

[30] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação, op. cit., p. 189.

Nessa perspectiva, é crucial que se tenha presente, que embora a proteção de dados tenha sido deduzida (associada), em diversos casos, do direito à privacidade (v.g., nos EUA, o conceito de *informational privacy*) ou, pelo menos, também do direito à privacidade, como no caso da Convenção Europeia de Direitos Humanos (nos termos da exegese do artigo 8º levada a efeito pela CEDH), o fato é que o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a uma determinada pessoa natural, sendo irrelevante à qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática[31].

O que se pode afirmar, sem temor de incorrer em erro, é que seja na literatura jurídica, seja na legislação e jurisprudência, o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade. Aliás, não é à toa que Bruno Ricardo Bioni alertou para o fato de que o entendimento, hoje amplamente superado, de que o direito fundamental à proteção de dados consiste em mera evolução do direito à privacidade, é uma "construção dogmática falha"[32].

2.2. Proteção de dados pessoais

Considerando que a definição corrente e legalmente consagrada de dados pessoais – cuja consistência constitucional não tem sido objeto de relevante contestação – é a de "informação relacionada a pessoa natural identificada ou identificável" (artigo 5º, I, LGPD), conceito praticado também pelo RGPD (artigo 4º, nº 1), a distinção entre dados e informações, parece não ser relevante do ponto de vista de sua proteção jurídico-constitucional, porquanto o que importa, ao fim e ao cabo, seria então a configuração dos requisitos legais referidos e não a forma mediante a qual se corporifica uma determinada informação[33].

Note-se, outrossim, que o conceito de dados pessoais, que constituem o objeto dos deveres de proteção estatais e das posições subjetivas dos indivíduos, é em regra definido pelo legislador infraconstitucional e, ao fim e ao cabo, também pelos órgãos regulatórios

[31] Cf., por todos, KARG, Moritz. Artikel 4, Nr. 1. *In*: SIMITIS, Spiros; HORNUNG, SPIECKER GENANNT DÖHMANN, Indra. *Datenschutzgesetz*. Baden-Baden: Nomos, 2019. p. 287-290.
[32] Cf. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento, op. cit., p. 95.
[33] Cf. KARG, Moritz. Artikel 4, Nr. 1, op. cit., p. 286-87.

em geral e mesmo pelo Poder Judiciário. O que importa, portanto, é que a definição legal seja constitucionalmente consistente e não desborde de sua finalidade.

Como já adiantado, tanto a nova LGPD quanto o RGPD (e, por via de consequência, nos ordenamentos jurídicos de todos os Estados da União Europeia), definem dados pessoais como "informação relacionada a pessoa natural identificada ou identificável" (artigo 5º, I, LGPD e artigo 4, nº 1, RGPD), o que aqui se retoma para o efeito de destacar a necessidade de avançar no detalhamento da definição e de seu alcance, visto que o texto legal também fornece dados para a delimitação do destinatário da proteção (sujeito ativo do direito à proteção de dados), ademais da relativa abertura – ainda que assim não o pareça, numa primeira mirada – das expressões identificada, mas especialmente "identificável".

3. Dimensão subjetiva e objetiva e multifuncionalidade do direito à proteção de dados pessoais

3.1. O direito à proteção de dados pessoais como direito subjetivo

Assim como se dá com os direitos fundamentais em geral, também o direito à proteção de dados pessoais apresenta uma dupla dimensão subjetiva e objetiva, cumprindo uma multiplicidade de funções na ordem jurídico-constitucional. Na sua condição de direito subjetivo e considerado como um direito em sentido amplo, o direito à proteção de dados pessoais se decodifica em um conjunto heterogêneo de posições subjetivas de natureza defensiva (negativa), mas também assume a condição de direito a prestações, cujo objeto consiste em uma atuação do estado mediante a disponibilização de prestações de natureza fática ou normativa[34].

Ainda em sede preliminar, é de se observar que, nada obstante a circunstância de que o direito à proteção de dados pessoais guarda relação direta (mas, como já adiantado, não se confunde) com um direito à autodeterminação informativa – que, de todo modo, é um dos esteios e elementos centrais da proteção de dados – na sua condição de direito subjetivo, o catálogo de posições jusfundamentais que encerra é bastante diversificado.

Nesse contexto, para melhor e mais rápida compreensão, calha lançar mão do rol de posições jurídicas subjetivas diretamente inspirado na obra de J.J. Gomes Canotilho e Vital Moreira, o qual, a despeito de eventuais diferenças de uma ordem jurídica para

[34] Cf. SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018. p. 288.

outra, se mostra perfeitamente compatível com o direito constitucional e infraconstitucional positivo brasileiro, assegurando uma proteção que dê conta de todas as dimensões que envolvem a coleta, armazenamento, tratamento, utilização e transmissão de dados pessoais:

a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos ou privados;
b) o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais;
c) o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados;
d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados;
e) o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados[35].

Note-se, ainda, que embora o direito à proteção de dados pessoais, como direito fundamental que é, tenha esteio na constituição, não há, no texto constitucional brasileiro (ao menos por ora) qualquer referência direta a posições jurídico-subjetivas específicas que possam estar albergadas por seu âmbito de proteção, o que, todavia, não quer dizer que não encontrem fundamento constitucional implícito.

De qualquer sorte, também no Brasil – e independentemente da incorporação de um direito à proteção de dados pessoais à CF – é na legislação infraconstitucional que foram especificados os direitos do titular da proteção, como dá conta o leque contido nos artigos 17 e 18 da LGPD, que, contudo, deve ser compreendido e aplicado em sintonia e conformidade com a CF, a normativa internacional e outros diplomas legais, como é o caso, por exemplo (e em especial) da Lei de Acesso à Informação e na Lei do Marco Civil da Internet.

Já mediante uma simples leitura do catálogo que segue, enunciado nos artigos 17 e 18 da LGPD, é possível perceber que em grande medida as posições jurídicas subjetivas (direitos) atribuídos ao titular dos dados pessoais objeto da proteção legal, que concretiza e delimita, em parte, o próprio âmbito de proteção do direito fundamental à proteção de dados, coincide com o rol de posições jurídico-constitucionais diretamente e habitualmente associadas à dupla função de tal direito como direito negativo (defesa) e positivo (a prestações).

[35] Cf. GOMES CANOTILHO, José Joaquim; MOREIRA, Vital. *Constituição da República Portuguesa anotada*, 4. ed. Coimbra: Coimbra Editora, 2007. p. 551 e ss.

Para tanto, segue a transcrição do catálogo legal referido, contido no capítulo III da LGPDB – "dos direitos do titular"[36]:

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, intimidade e de privacidade, nos termos desta lei.
>
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I. confirmação da existência de tratamento;
> II. acesso aos dados;
> III. correção de dados incompletos, inexatos ou desatualizados;
> IV. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V. portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII. informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII. informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX. revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
>
> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".
>
> Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
>
> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em Juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Note-se, ainda, que a lista de posições jurídicas supra não tem caráter taxativo, não excluindo, portanto, outras possibilidades, mesmo que não expressamente positivadas na constituição ou num diploma legal. Outrossim, é possível perceber uma considerável simetria entre o catálogo de direitos do usuário da LGPD e do RGPD (artigo 17), de tal

[36] Convém alertar que não se está a transcrever todos os dispositivos contidos no capítulo III da LGPDB, mas sim, os artigos que enunciam as posições jurídicas (direitos) propriamente ditos dos titulares dos dados pessoais.

sorte que as diferenças em regra se limitam a variações terminológicas, no sentido de maior ou menor precisão da nomenclatura utilizada.

Todavia, existe, como já referido, espaço para o reconhecimento de outras posições jurídicas, como se dá, em caráter ilustrativo, com o assim chamado direito ao esquecimento. Neste caso, embora algumas de suas expressões (no sentido de instrumentos de efetivação) se encontrem especificadas nos textos legais colacionados (v.g. os direitos ao apagamento, retificação), outras carecem de acolhimento pelas instâncias legiferantes, pelo Poder Judiciário ou mesmo pelos próprios atores da internet, mediante autorregulação. Nesse contexto, o melhor exemplo talvez seja o de um direito à desindexação relativamente aos provedores de pesquisa na internet, que, a despeito da controvérsia que grassa em torno do tema, tem sido objeto de reconhecimento em diversas decisões judiciais, sejam de tribunais nacionais, seja no plano supranacional, como é o caso do TJUE (caso "Google", 2014)[37].

De outra parte, calha referir, visto corresponder a uma espécie de "tradição" na esfera da prática legislativa brasileira, que também a LGPD, como se verifica mediante um breve olhar sobre o catálogo de direitos apresentado, acabou reproduzindo direitos já consagrados expressamente na CF e que, em virtude disso e por serem dotados de aplicabilidade imediata, não precisariam constar na esfera infraconstitucional, como é o caso dos direitos de liberdade, intimidade e privacidade (artigo 17) e do direito de acesso à Justiça (artigo 22).

3.2. A dimensão objetiva: deveres de proteção e de organização e procedimento

O "descobrimento" e o desenvolvimento da assim chamada dimensão objetiva dos direitos fundamentais – como já é de amplo conhecimento – pode ser reconduzido ao labor da doutrina e da jurisprudência constitucional alemãs, notadamente a partir da Década de 1950, ainda que as bases de tal concepção possam ser encontradas já no período da República de Weimar. Nesse contexto, sempre é recordada a paradigmática afirmação do Tribunal Constitucional Federal, no sentido de que os direitos fundamentais não se limitam à função precípua de serem direitos subjetivos de defesa do indivíduo contra atos do poder público, mas que, além disso, constituem decisões valorativas de

[37] Sobre o direito ao esquecimento no Brasil e no direito estrangeiro e internacional, remetemos, em língua portuguesa, a SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. *O Direito ao "Esquecimento" na Sociedade de Informação*. Porto Alegre: Livraria do Advogado, 2018.

natureza jurídico-objetiva da Constituição, com eficácia em todo o ordenamento jurídico e que fornecem diretrizes para os órgãos legislativos, judiciários e executivos[38].

Todavia, também convém relembrar que a perspectiva objetiva dos direitos fundamentais não representa um mero "reverso da medalha" da perspectiva subjetiva, mas sim, significa que às normas que preveem direitos subjetivos é outorgada função autônoma, que transcende esta perspectiva subjetiva[39] e que, além disso, desemboca no reconhecimento de conteúdos normativos e, portanto, de funções distintas aos direitos fundamentais[40].

Dentre tais funções e conteúdos normativos, três são particularmente relevantes em virtude do seu impacto no campo da proteção dos direitos fundamentais, inclusive e mesmo prioritariamente na sua condição de direitos subjetivos.

A primeira – embora as críticas endereçadas especialmente à terminologia utilizada – diz com o assim chamado efeito (eficácia irradiante – *Ausstrahlungswirkung*) dos direitos fundamentais, no sentido de que esses, na sua condição de direito objetivo, fornecem impulsos e diretrizes para a aplicação e interpretação do direito infraconstitucional, o que, além disso, apontaria para a necessidade de uma interpretação conforme aos direitos fundamentais, que, ademais, pode ser considerada – ainda que com restrições – como modalidade semelhante à difundida técnica hermenêutica da interpretação conforme à Constituição[41].

Associado a tal efeito, encontra-se a assim chamado fenômeno da constitucionalização do Direito, incluindo o direito privado, assim como a problemática da eficácia dos direitos fundamentais nas relações privadas, também abordada sob a denominação de eficácia horizontal, ou *Drittwirkung* (eficácia em relação a terceiros).

---

[38] Cf. *BVerfGE 7*, 198/204 e ss., posteriormente objeto de ratificação em outras decisões (por ex., *BVerfGE 49*, 89/141 e ss.).

[39] Cf., dentre tantos, ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. Coimbra: Almedina, 1987. p. 143.

[40] Neste sentido, por exemplo, DREIER, Horst. Subjektiv-rechtliche und objektiv-rechtliche Grundrechtsgehalte. *JURA*, 1994. p. 509.

[41] V., dentre outros, PIEROTH, Bodo; SCHLINK, Bernhard. *Grundrechte*. Staatsrecht II. 11. ed. Heidelberg: C. F. Müller, 1995. p. 23. No direito lusitano estes efeitos da dimensão objetiva encontram-se arrolados de forma clara e didática na obra de ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, op. cit., p. 168-9, que, neste contexto, além da necessidade de uma interpretação conforme os direitos fundamentais, aponta, ainda, para a existência de uma obrigação geral de respeito vigente também na esfera privada e que identifica como um efeito externo deles. Neste sentido, entendemos que este dever geral de respeito tanto diz respeito à necessidade de uma hermenêutica vinculada aos direitos fundamentais, quanto à problemática de sua eficácia privada.

Nesse contexto, é de sublinhar que que a ideia de os direitos fundamentais irradiarem efeitos também nas relações privadas e não constituírem apenas direitos oponíveis aos poderes públicos vem sendo considerada um dos mais relevantes desdobramentos da perspectiva objetiva dos direitos fundamentais e será abordada logo mais adiante, na parte relativa aos destinatários dos direitos fundamentais.

Outra importante função atribuída aos direitos fundamentais e desenvolvida com base na existência de um dever geral de efetivação atribuído ao Estado, por sua vez agregado à perspectiva objetiva dos direitos fundamentais, diz com o reconhecimento de deveres de proteção (*Schutzpflichten*) do Estado, no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos não somente contra os poderes públicos, mas também contra agressões provindas de particulares e até mesmo de outros Estados[42].

Assim, se é correto – como leciona Dieter Grimm – que os deveres de proteção, por exigirem intervenções por parte dos órgãos estatais – resultam em restrições de direitos, acarretando, nesta perspectiva, uma redução do âmbito de liberdade individual, tais restrições, vinculadas precisamente à necessidade de proteção de bens fundamentais (além de sujeitas, convém acrescentar, ao regime dos limites dos limites dos direitos fundamentais, nomeadamente, o respeito às exigências da proporcionalidade e da garantia do núcleo essencial) têm sempre por escopo a maximização dos direitos fundamentais, visto que as restrições objetivam, no plano geral, mais proteção da liberdade e dos direitos fundamentais das pessoas no âmbito da comunidade estatal[43]. Assim, os deveres de proteção não constituem – na dicção de Gomes Canotilho – "um simples dever de acção do Estado para proteger bens ou promover fins constitucionais, mas de um dever de acção para 'segurar' direitos consagrados e protegidos por normas constitucionais"[44].

Importa agregar, outrossim, que uma das peculiaridades dos deveres de proteção reside no fato de que são múltiplos os modos de sua realização, que pode se dar, por meio de normas penais, do estabelecimento da responsabilidade civil, de normas procedimentais, de atos administrativos e até mesmo por uma atuação concreta dos

---

[42] A este respeito, v., dentre outros, HESSE, Konrad. *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*. 20. ed. Heidelberg: C. F. Müller, 1995. p. 155.

[43] Cf. GRIMM, Dieter. A função protetiva do Estado. *In*: SOUZA NETO, C. P.; SARMENTO, D. *A Constitucionalização do Direito*. Rio de Janeiro: Lumen Juris, 2007. p. 160.

[44] Cf. GOMES CANOTILHO, José Joaquim. Omissões normativas e deveres de proteção. *In*: DIAS, Jorge de Figueiredo (Coord.). *Estudos em homenagem a Cunha Rodrigues* Coimbra: Coimbra Editora, 2001. v. II. p. 113.

poderes públicos[45]. Por outro lado, a forma como o Estado assume os seus deveres de proteção, e os efetiva, permanece em primeira linha, no âmbito de seu próprio arbítrio, levando-se em conta, nesse contexto, a existência de diferentes alternativas de ação, a limitação dos meios disponíveis, a consideração de interesses colidentes e a necessidade de estabelecer prioridades, de tal sorte que não se poderia, em princípio, falar de um dever específico de agir por parte do Estado[46].

Como último importante desdobramento da perspectiva objetiva – a função outorgada aos direitos fundamentais sob o aspecto de parâmetros para a criação e constituição de organizações (ou instituições) estatais e para o procedimento[47]. Nesse contexto, há que considerar a íntima vinculação entre direitos fundamentais, organização e procedimento, no sentido de que os direitos fundamentais são, ao mesmo tempo e de certa forma, dependentes da organização e do procedimento (no mínimo, sofrem uma influência da parte destes), mas simultaneamente também atuam sobre o direito procedimental e as estruturas organizacionais[48].

Tendo em vista que os deveres de proteção do Estado podem, por vezes, concretizar-se por meio de normas dispondo sobre o procedimento administrativo ou judicial, bem como pela da criação de órgãos, constata-se, desde já, a conexão que pode existir entre estas duas facetas da perspectiva jurídico-objetiva dos direitos fundamentais[49]. Para além desta constatação, foi feita oportuna referência na doutrina para a necessidade de um procedimento ordenado e justo para a efetivação ou garantia eficaz dos direitos fundamentais[50].

---

45 Cf., novamente, ALEXY, Robert. *Theorie der Grundrechte*. 2. ed. Frankfurt a.M. Suhrkamp, 1994. p. 410. Inobstante já tenha sido anunciada em decisões anteriores, a problemática do reconhecimento de deveres de proteção por parte do Estado foi objeto de formulação mais exaustiva na paradigmática decisão do Tribunal Constitucional Federal da Alemanha sobre a descriminação do aborto (Abtreibungsurteil: *BVerfGE* 39,1), na qual, com base no direito à vida (art. 2, inc. II, da Lei Fundamental), foi deduzida uma obrigação do Estado no sentido de proteger a vida humana em geral, incluindo a vida em formação, independentemente da possibilidade de o nascituro ser ele próprio titular de direitos fundamentais, revelando, neste contexto, o desenvolvimento da teoria dos deveres de proteção com base na perspectiva objetiva dos direitos fundamentais. Neste sentido, cf. STERN, Klaus. Idee und Elemente eines Systems der Grundrechte. *In:* KIRCHHOF, J. Isensee-P. (Coord.). *Handbuch des Staatsrechts der Bundesrepublik Deutschland*. Heidelberg: C. F. Müller, 1992. v. 5. p. 80.

46 Neste sentido, representando a posição majoritária na doutrina, as lições de MANSSEN, Gerrit. *Staatsrecht I Grundrechtsdogmatik*. München: Verlag Franz Vahlen, 1995. p. 18, PIEROTH, Bodo; SCHLINK, Bernhard. *Grundrechte*. Staatsrecht II, op. cit., p. 27, bem como de HESSE, Konrad. *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*, op. cit., p. 156.

47 Neste sentido, dentre tantos, JARASS, Hans; PIEROTH, Bodo. *Grundgezetz fur die Bundesrepublik Deutschland*: Kommentar. München: C. H. Beck. 13. Auf. 2014. p. 20.

48 Cf. HESSE, Konrad. *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*, op. cit., p. 160-1.

49 Cf, por todos, PIEROTH, Bodo; SCHLINK, Bernhard. *Grundrechte*. Staatsrecht II, op. cit., p. 27.

50 Na literatura brasileira, remetemos às formulações de SARLET, Ingo Wolfgang; MARINONI, Luiz

Ainda no que diz com a perspectiva procedimental (de que a proteção dos direitos fundamentais depende de estruturas organizacionais e de procedimentos adequados), há que sublinhar a necessidade de utilização e otimização de técnicas processuais que assegurem, com o maior nível possível de eficácia, a proteção dos direitos fundamentais, o que, dada a natureza/função dos direitos e das circunstâncias que envolvem a sua incidência em casos concretos, pode implicar técnicas distintas para direitos distintos mas também técnicas diversas para a proteção do mesmo direito fundamental[51].

Que isso se revela particularmente importante para o caso do direito à proteção de dados pessoais não é difícil perceber desde logo, posto que – dado o desenvolvimento de novas tecnologias de informação e comunicação – o desafio da efetividade dos direitos, inclusive e em especial dos mecanismos convencionais para a sua realização (direito sancionatório, processo judicial e a eficácia de suas decisões etc.) é imenso, questão que aqui contudo, não temos como desenvolver, bastando relembrar aqui, em caráter ilustrativo, o fenômeno da onipresença da digitalização e de seu impacto sobre os direitos de personalidade, o problema da ausência real de fronteiras territoriais etc.

Ainda nessa quadra, é de se enfatizar que o Estado dispões de várias alternativas para dar conta dos seus deveres de proteção, que vão desde a criminalização de ações e omissões, responsabilidade civil, instituição de mecanismos processuais, como é o caso, no Brasil, da ação de *habeas data*, até a criação de órgãos (organismos) público e/ou privados encarregados de levar a efeito os deveres de proteção, designadamente, no que interessa aqui, a criação e estruturação da Autoridade Nacional de Proteção de Dados – ANPD (arts. 55-A – 55-L), a exemplo do que se deu em outros lugares.

4. Titulares e destinatários do direito (e correspondentes deveres de proteção) à proteção de dados

4.1. Titularidade

A noção de direito subjetivo, também no tocante aos direitos fundamentais, envolve (além da exigibilidade) uma relação trilateral entre o titular (ou sujeito ativo), o objeto e o

Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. 3. ed. São Paulo: Revista dos Tribunais, 2014.

[51] Sobre o tema, v., no Brasil, em especial, MARINONI, Luiz Guilherme. *Técnica processual e tutela dos direitos*. 4. ed. São Paulo: Revista dos Tribunais, 2013.

destinatário (sujeito passivo) do direito – posição(ções) jurídica(s) – atribuída(s) pelo direito objetivo[52].

No caso do direito à proteção de dados pessoais – acordo com a legislação respectiva (no caso brasileiro, o artigo 5º da LGPD), os titulares do direito são, em primeira linha, as pessoas naturais (identificadas e identificáveis, como visto acima).

Isso, contudo, não significa, por si só, que todas as pessoas naturais sejam titulares de direitos fundamentais, o que também se dá com a proteção de dados, visto que a titularidade de posições jurídicas subjetivas por parte de pessoais naturais pode variar conforme alguns critérios, por exemplo, a cidadania, a idade, eventual incapacidade por força de alguma deficiência.

No caso da CF, a despeito do disposto no artigo 5º, *caput*, de que são titulares dos direitos fundamentais os brasileiros e estrangeiros residentes no país, doutrina e jurisprudência de há muito tem ampliado o leque de sujeitos ativos em um número significativo de casos, incluindo os direitos de personalidade, e, por conseguinte, também do direito à proteção de dados pessoais, o que, por ser algo consolidado, aqui se deixa de desenvolver.

Nesse sentido – mas não por este – como já lembrado, o direito à proteção de dados, sendo direito de todos e de qualquer um, é também um direito humano.

Em homenagem à clareza, calha reproduzir – de novo – o disposto no artigo 1º da LGPD, que, somando-se ao que prescreve o já citado artigo 5º da lei, assim reza:

> "Art. 1º Esta Lei *dispõe sobre o tratamento de dados pessoais*, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o *objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural* (grifos nossos)".

É claro que a opção legal é passível de contestação, designadamente, se incompatível com o marco constitucional, mas, desde que assegurada – ainda que por outro fundamento – a proteção de dados das pessoas jurídicas, e, ao mesmo tempo, garantida a proteção dos dados pessoais dos respectivos sócios, na condição de pessoas naturais (assim como dos dados pessoais de terceiros), não se vislumbra, salvo melhor

[52] GOMES CANOTILHO, José Joaquim. Omissões normativas e deveres de proteção, op. cit., p. 544. SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*, op. cit., 2014. p. 353.

juízo, razão suficientemente robusta para justificar a ilegitimidade jurídica de tal distinção.

Todavia, para não transmitir a ideia de que desconhecemos a existência de tal posição, calha referir linha de argumentação que tem tido já alguma representatividade, embora ainda mais embrionária, e que poderia dar sustentáculo à proteção de dados equivalente a dos dados de pessoais naturais, em virtude de se atribuir às pessoas jurídicas a titularidade do direito à privacidade, agregando-se o fato de que a proteção de dados tem um cunho instrumental, servindo, em primeira linha, à salvaguarda da própria privacidade[53].

Mas também as pessoas jurídicas e entes sem personalidade jurídica, desde que, nos dois últimos casos, o acesso, conhecimento, utilização e difusão dos dados que tenham sido armazenados possam afetar direitos e interesses de terceiros, no caso, de pessoas naturais[54], mas há quem prefira proteger os dados da pessoa jurídica por conta do segredo empresarial[55].

De qualquer sorte, como já adiantado, entendemos que a opção legislativa guarda a harmonia e simetria necessária com os marcos normativos mais relevantes para o sistema brasileiro, em especial o Regulamento Geral de Proteção de Dados da Europa, que, de resto, foi em boa parte recepcionado pelo nosso legislador e já havia encontrado ressonância nos trabalhos preparatórios de elaboração do projeto de lei.

De todo modo, ainda que sejamos adeptos da posição, por ora dominante no cenário doutrinário, legislativo e jurisprudencial, de que o direito à proteção de dados pessoais tem por titulares apenas pessoas naturais, não se está a negar – como, de resto, já adiantado e amplamente aceito na doutrina (inclusive de nossa lavra) e jurisprudência constitucional, mas também em diversos textos constitucionais – que as pessoas jurídicas e mesmo outros entes não sejam titulares de direitos fundamentais, compatíveis, é claro (como, aliás, também prescreve o artigo 52 do Código Civil Brasileiro) com a sua condição, o que, contudo, se verifica caso a caso.

---

53 Sobre o tema da atribuição da titularidade de direitos de personalidade às pessoas jurídicas, inclusive do direito à privacidade e em certa medida da proteção de dados, v., na literatura brasileira, a atual e excelente contribuição de ANDRADE, Fábio Siebeneichler de. Notas sobre a aplicabilidade dos direitos da personalidade à pessoa jurídica como evolução da dogmática civil. *RJLB*, a. 4, n. 5, p. 806-837, 2018, especialmente p. 817 e ss., sublinhando-se que o autor retrata a evolução da discussão no direito comparado, apresentando e sopesando argumentos favoráveis e contrários, à luz de exemplos extraídos da legislação e jurisprudência, além de atualizada e relevante revisão doutrinária.

54 Cf., por todos, IPSEN, Jörn. *Staatsrecht II – Grundrechte*. 17. Auf. Vahlen, 2014. p. 78.

55 Cf. é o caso de KLOEPFER, Michael. *Verfassungsrecht II*. München: C. H. Beck. 13. Auf. 2010. p. 156.

Assim, não sendo o enfrentamento desse ponto central para a presente contribuição, cuida-se, de todo modo, de tema atual e que exige ser levado a sério. Especificamente no que concerne à proteção de dados e considerando que as pessoas jurídicas já são protegidas, inclusive na perspectiva jusfundamental, por outros direitos e garantias (sigilo industrial e comercial, propriedade imaterial etc.), é questionável que com a inclusão das pessoas jurídicas no polo subjetivo ativo dos direitos à privacidade e intimidade, bem como do direito à proteção de dados pessoais, implique em ganho real qualitativo de proteção.

Além disso, é de se questionar se tal reconhecimento, caso venha a prevalecer, não poderia ensejar a diminuição dos níveis (já de fato não muito robustos) de proteção dos dados pessoais das pessoas naturais, o que também aqui não será desenvolvido.

Ainda sobre o ponto, mesmo que a proteção de dados pessoais como tal seja assegurada apenas às pessoas naturais, o mesmo não ocorre com a titularidade do direito à autodeterminação informativa, que, embora aqui também se verifique controvérsia, tem sido, pelo menos em algumas ordens jurídicas – como é o caso, na Alemanha, por força de orientação fixada pelo Tribunal Constitucional Federal – atribuído igualmente às pessoas jurídicas[56].

Isso, embora possa soar contraditório – e de fato o é se em questão estivesse a proteção apenas de dados pessoais sensíveis –, acaba sendo uma solução no limite coerente quando se reconhece ao direito à autodeterminação informativa um âmbito de proteção mais amplo do que ao da proteção de dados pessoais, no sentido de que qualquer um (pessoa jurídica ou natural, e mesmo entes despersonalizados) é titular da liberdade de se autodeterminar em relação aos dados que lhe "pertencem", sejam, ou não, dados pessoais de acordo com a respectiva legislação protetiva. De todo modo, não é o caso aqui de avançar com a discussão.

[56] Cf., por todos, DREIER, Horst. Art. 2 I – allgemeines Persönlichkeitsrecht. *In*: DREIER, Horst (Coord.). *Grundgesetz Kommentar*. 3. Auf. Tübingen: Mohr Siebeck, 2013. p. 386-8, mediante referência ao julgado do Tribunal Constitucional Federal respectivo (*BVerfGE* 118, p. 202 e ss.), destacando-se. No mesmo sentido, igualmente destacando a existência de controvérsia sobre o tema e da mesma forma ressalvando que o Tribunal Constitucional Federal não admite, para efeito da titularidade de direitos de personalidade por parte de pessoas jurídicas seja invocada a dignidade humana, v., mais recentemente, MURSWIEK, Dietrich; RIXEN, Stephan. Persönliche Freiheitsrechte. *In:* SACHS, Michael. *Grundgesetz Kommentar*. 8. ed. München: C.H.Beck, 2018. p. 132.

4.2. Destinatários

Destinatários do direito (vinculados pelo direito) são tanto o Estado quanto os particulares, pois a devassa da vida privada, incluindo o acesso e utilização de dados pessoais, é algo que atualmente decorre tanto de ações (ou, a depender do caso, de omissões) de órgãos e agentes estatais quanto das de entidades privadas ou pessoas físicas.

4.2.1 Órgãos estatais: legislativo, executivo e judiciário

No direito constitucional e na dogmática dos direitos fundamentais brasileira é absolutamente majoritário o entendimento de que os direitos fundamentais, o que, à evidência, se aplica ao direito à proteção de dados, vinculam diretamente, na condição de normas imediatamente aplicáveis, todos os atores (órgãos, funções, agentes, atos) estatais, aqui considerados em sentido amplo, de modo a assegurar uma proteção sem lacunas[57].

Isso significa, em síntese, que tais atores devem, no âmbito e limites de suas respectivas funções, competências e atribuições, aplicar e concretizar o direito à proteção de dados, assegurando-lhe a sua máxima eficácia e efetividade concreta, tanto na condição de direito subjetivo negativo (não intervenção arbitrária no seu âmbito de proteção), quanto, por força de sua dimensão objetiva, levando a sério os respectivos deveres de proteção e o critério da proibição de proteção insuficiente[58].

Muito embora não exista um meio específico a ser adotado para dar conta dos deveres de proteção do Estado, no tocante à proteção de dados e aos direitos de personalidade que lhe são correlatos, o mais atual e relevante exemplo no Brasil – levado a efeito pelo Poder Legislativo – é o da edição da LGPD e seu sistema de garantias materiais e processuais, incluindo a autoridade nacional de proteção de dados, sem deixar de considerar aqui diplomas anteriores onde a proteção de dados também foi objeto de previsão, tais como o *Código de Defesa do Consumidor*, *O Marco Civil da Internet*, a *Lei de Acesso à Informação* e a ação constitucional do *Habeas Data*.

Outrossim, assumem relevo como meios de concretização dos deveres de proteção pelo Poder Legislativo (e aqui também, nos limites de suas competências, do Poder Executivo), a eventual criminalização de violações dos direitos fundamentais relevantes

[57] Cf., por todos, SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional, op. cit, p. 272.
[58] SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional, op. cit, p. 414 e ss.

em matéria de proteção de dados, a responsabilidade civil de particulares e do Estado, instrumentos processuais adequados, dotação orçamentária suficiente, entre outros.

O Poder Judiciário, a quem incumbe inclusive o controle do cumprimento dos deveres de proteção pelos demais órgãos estatais (tanto no nível da proibição do excesso de intervenção quanto da insuficiência de proteção), já contribuiu e tem contribuído em diversos aspectos, como, por exemplo, ao reconhecer um direito fundamental à proteção de dados e um direito a autodeterminação informativa, ainda que se possa afirmar que se trata de institutos (ainda – em parte) carentes de maior delimitação e desenvolvimento dogmático, em especial na própria seara jurisdicional, mas também doutrinário-acadêmica, nada obstante a existência já de relevantes estudos sobre o tema no Brasil[59].

4.2.2 Particulares: o problema da eficácia do direito fundamental à proteção de dados pessoais na esfera das relações privadas

A partir do exame da assim chamada dimensão objetiva dos direitos fundamentais, verificou-se que uma de suas projeções e consequências jurídicas reside naquilo que foi chamado de uma eficácia irradiante dos direitos fundamentais, no sentido que os valores por eles exprimidos devem iluminar toda a ordem jurídica, mediante a sua constitucionalização, que abarca também uma consideração de tais parâmetros na esfera das relações jurídicas entre atores privados.

Note-se, ainda nessa fase preliminar, que a existência de uma vinculação dos particulares aos direitos fundamentais foi, mediante processos nem sempre coincidentes nos diferentes sistemas jurídicos, reconhecida, de modo generalizado, pelo menos no direito continental europeu, sul-americano e mesmo em outras regiões, de tal sorte que é possível partir da premissa de que a pergunta sobre o "se" de uma eficácia dos direitos fundamentais nas relações privadas foi respondida positivamente o que também é, como amplamente reconhecido, o caso do Brasil.

De outra parte, contudo, quanto ao modo (o "como") pelo qual se dá tal vinculação e eficácia ainda não existe consenso, seja na literatura, seja em nível jurisprudencial, ademais da falta de consistência e de parâmetros seguros para o seu manejo que se verifica em um não raro número de casos.

Além disso, é de se adiantar que a eficácia dos direitos fundamentais na esfera das relações privadas se dá de modo diferenciado, poderíamos dizer, em perspectiva

[59] Dentre as contribuições que se destacam sobre o tema, v. os já citados Danilo Doneda, Têmis Limberger, Regina Ruaro, Laura Mendes, Fabiano Menke e Bruno Ricardo Bioni.

multinível, visto que se trata de algo que se passa no campo do direito internacional público (tendo em conta o reconhecimento, pela doutrina e jurisprudência dos tribunais internacionais, de uma vinculação dos particulares aos direitos humanos), bem como nas ordens jurídicas nacionais. Para o caso da proteção de dados, que envolve massivamente atores privados, não é preciso maior esforço para demonstrar que o problema se revela particularmente atual e relevante.

Nesse contexto, note-se que a despeito da influência da doutrina e jurisprudência alemã no que diz com a dogmática dos direitos fundamentais, a doutrina predominante na Alemanha, de uma eficácia em regra mediata (indireta) dos direitos fundamentais nas relações privadas[60], tem sido mesmo lá parcialmente repensada e ajustada (inclusive pelo Tribunal Constitucional Federal)[61], além de não ter sido adotada (ainda que por vezes mais do ponto de vista teórico do que prático) em outros ambientes, como é o caso do Brasil, por exemplo, onde (ainda) prevalece a tese de uma eficácia em princípio direta, ainda que se registrem importantes diferenças entre as concepções adotadas entre os autores que se tem dedicado ao tema[62].

De qualquer sorte, também os que advogam uma eficácia em princípio direta convergem quanto ao fato de que não se cuida de uma eficácia absoluta, mas que exige uma metódica diferenciada, que leve em conta em primeira linha as opções legislativas e

---

[60] Cf. por todos, CANARIS, Claus-Wilhelm. *Grundrechte und Privatrecht.* Berlin-New York: Walter de Gruyter, 1999, embora se deva referir que o autor, em conferência realizada no Brasil, na Pontifícia Universidade Católica, Porto Alegre em 2012, publicada na Revista Direitos Fundamentais & Justiça (Ano 07, vol. 22), tenha sustentado que, em se tratando de proibições de discriminação vinculadas à proteção da dignidade humana, uma eficácia direta se revela cogente. V. CANARIS, Claus-Wilhelm. Considerações a respeito da posição de proibições de discriminação no Sistema de Direito Privado. *Revista Direitos Fundamentais e Justiça*, a. 7, n. 22, jan./mar. 2013. p. 15-20.

[61] Cf., por último, RUFFERT, Matthias. *Privatrechtswirkung der Grundrechte. Von Lüth zum Stadionverbot – und darüber hinaus?*. n. 1, Jus 2020. p. 1-12, apresentando os últimos desenvolvimentos e tendências, em especial na jurisprudência do Tribunal Constitucional Federal da Alemanha.

[62] Representativos de uma eficácia direta, mas não absoluta, e respeitando em primeira linha as opções legislativas v., em ordem cronológica e dentre os autores de direito constitucional, em especial, SARLET, Ingo Wolfgang. Direitos Fundamentais e Direito Privado, algumas considerações em torno da vinculação dos particulares aos direitos fundamentais. *In*: SARLET, Ingo Wolfgang (Coord.). *A Constituição Concretizada: Construindo Pontes para o Público e o Privado*. Porto Alegre: Livraria do Advogado, 2000. p. 107-163; STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais*. São Paulo: Malheiros, 2004; SARMENTO, Daniel. *Direitos Fundamentais e Relações Privadas*. Rio de janeiro: Lumen Juris, 2003. Sugerindo modelo alternativo v. SILVA, Virgílio Afonso da. *A Constitucionalização do Direito.* Os direitos fundamentais nas relações entre particulares. São Paulo: Malheiros, 2005. Mas, há também quem refute categoricamente uma eficácia direta afirmando que a influência dos direitos fundamentais nas relações privadas se dá apenas de modo indireto, como é o caso, no Brasil, de DIMOULIS, Dimitri; MARTINS, Leonardo. *Teoria Geral dos Direitos Fundamentais*. São Paulo: RT, 2007. p. 104 e ss. e DUQUE, Marcelo Schenk. *Direito Privado e Constituição.* Drittwirkung dos Direitos Fundamentais. Sâo Paulo: Revista dos Tribunais, 2013, assim como, mais recentemente, RODRIGUES JÚNIOR, Otávio Luís. *Direito Civil Contemporâneo*: Estatuto Epistemológico, Constituição e Direitos Fundamentais. 2. ed. São Paulo: GEN, 2019.

a necessidade de cuidadosa ponderação no caso concreto, v.g. avaliando a existência de uma assimetria entre os atores e as posições em choque, bem como atendendo os critérios do teste de proporcionalidade, designadamente na solução de colisões entre direitos fundamentais, como ocorre também no caso do direito fundamental à proteção de dados pessoais.

No que diz com a jurisprudência do STF sobre o tema, este, por maioria de votos, reconheceu uma eficácia direta, entendendo que o direito ao devido processo legal, em especial a garantia do contraditório, se aplica também às relações privadas. No caso concreto, tratava-se de anular a exclusão de um integrante (associado) da União Brasileira de Compositores, que havia sido afastado sem que lhe tivesse sido assegurada a possibilidade de ser ouvido e se defender, inexistindo regulação legal específica. Chama a atenção, no caso, que o STF também levou em conta elementos da *state action doctrin* norte-americana, ainda que naquele sistema jurídico a vinculação dos atores privados seja em regra refutada[63]. Nesse sentido, cabe sublinhar que um dos esteios da argumentação residiu no fato de que a União Brasileira de Compositores, embora tenha a natureza de uma pessoa jurídica de direito privado, exerce uma função de natureza pública e de interesse público, o que implica uma incidência mais forte dos direitos fundamentais[64].

Muito embora uma eficácia direta não tenha sido limitada às situações em que se verifica um desequilíbrio de condições e entre as partes envolvidas no conflito, em virtude da existência de atores privados poderosos (que tem maior capacidade de influir mesmo o processo legislativo ou a ação estatal em geral) ou que exercem atividades que podem ser em parte equiparadas ao reconduzidas ao Estado, no caso da proteção de dados e, da mesma forma, no ambiente digital, esse fato assume uma relevância peculiar e que deve pautar o entendimento com relação ao tema. Em especial trata-se de aspecto a ser levado em conta quando da ponderação (balanceamento) que precisa ser levada a efeito pelo Juiz na solução dos conflitos.

No caso do direito fundamental à proteção de dados pessoais, isso é de especial relevância, em virtude do poder econômico e social, mas também político, exercido por

---

[63] Sobre a doutrina da *state action* nos EUA v., por todos, BILBAO UBILLOS, Juan Maria. *Los derechos fundamentales en la frontera entre lo público y lo privado.* La noción de "state action" en la jurisprudencia norteamericana. Madrid: McGraw-Hill, 1997.

[64] V. Recurso Extraordinário 201819/RJ. BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário: RE 201819/RJ.* Ministro Relator para o Acórdão: Gilmar Mendes. Julgado em: 11.10.2005. Disponível: http://stf.jus.br/portal/processo/verProcessoAndamento.asp?numero=201819&classe=RE&codigoClasse=0&origem=JUR&recurso=0&tipoJulgamento=M. Acesso em: 06 fev. 2018
.

grandes corporações, gerando um grande desequilíbrio entre as partes envolvidas na teia de relações jurídicas que se estabelecem. Além disso, não se deve desconsiderar que quanto aos dados pessoais, ainda mais em se tratando do mundo digital, a exigência do consentimento do titular dos dados e usuário das tecnologias de informação (aplicativos de toda ordem, mídias sociais, compras pela internet etc.), embora cogente do ponto de vista constitucional e legal, esbarra de modo substancial – ainda que diferenciada – nas limitações à autonomia privada.

Isso se deve especialmente ao fato de a ampla maioria dos bens e serviços disponibilizados apenas serem acessíveis aos usuários mediante contratos de adesão, sem falar na circunstância de que, em virtude da necessidade gerada no sentido da utilização de diversos desses serviços, em muitos casos se estabelece praticamente uma obrigação (fática) de contratar que, por sua vez, literalmente esvazia a autonomia individual e o direito fundamental à livre autodeterminação informativa, ancorados na CF e também previstos na legislação ordinária, em especial – no que interessa ao presente texto – na legislação para a proteção dos dados pessoais[65].

Por tais razões, também no tocante à proteção dos dados pessoais, seja em que contexto for, mas em especial no ambiente digital, não se pode admitir uma esfera de atuação privada completamente livre dos direitos fundamentais[66], gerando uma espécie de imunidade, tanto mais perigosa – no que concerne a violações de direitos – quanto mais força tiverem os atores privados que operam nesse cenário. Por isso, um controle rigoroso das restrições a direitos fundamentais na esfera das relações privadas, inclusive em caráter preventivo, levando em conta os deveres de proteção estatais também em face de perigos e riscos, é de ser levado a efeito (inclusive!) pelos Tribunais[67]. Tal controle, contudo, deve levar a sério, em primeira linha, as opções legislativas, mas ao mesmo tempo, não hesitar quando se trata de reconhecer e declarar eventual

[65] V., dentre tantos, HOFMANN-RIEM, Wolfgang. Reclaim Autonomy: Die Macht digitaler Konzerne. *In*: AUGSTEIN, Jakob (Coord.). *Reclaim Autonomy. Selbstermächtigung in der digitalen Weltordnung*. Frankfurt am Main: Suhrkamp, 2017. p. 121-142.

[66] Cf., por todos, FACHIN, Luiz Edson; RUZYK, Carlos Eduardo Pianovski. Direitos fundamentais, dignidade da pessoa humana e o novo código civil: uma análise crítica. *In*: SARLET, Ingo Wolfgang (Coord.). *Constituição, direitos fundamentais e direito privado*. Porto Alegre: Livraria do Advogado, 2003. p. 100 e ss., bem recordando que no Estado Democrático de Direito a função da Constituição não é mais apenas de operar como estatuto jurídico do político, mas sim, como parâmetro material integrador das esferas pública e privada, tendo como esteio a dignidade da pessoa humana e os direitos fundamentais.

[67] Cf., numa perspectiva mais ampla, REINHARDT, Jörn. Conflitos de direitos fundamentais entre atores privados: "efeitos horizontais indiretos" e pressupostos de proteção de direitos fundamentais. *Direitos Fundamentais & Justiça*, ano 13, n. 41, p. 59-91, jul./dez. 2019. Outrossim, calha frisar, não se está a dizer com isso que o papel principal deva ser exercido pelo Poder Judiciário, mas que existem casos que não podem (e não devem) ser subtraídos ao controle judicial.

inconstitucionalidade, pois, do contrário, a proteção dos dados pessoais poderá estar comprometida.

Por sua vez – à vista da circunstância de que a aplicação dos direitos fundamentais às relações privadas envolve conflitos entre direitos – é de se sublinhar que na solução dos casos submetidos ao controle judicial, imprescindível ser consistente com as exigências do teste de proporcionalidade, não apenas no sentido da proibição de uma intervenção (restrição) excessiva do âmbito de proteção do direito fundamental afetado, mas também – como decorrência dos deveres de proteção – no sentido da proibição de uma proteção insuficiente de um ou de alguns dos direitos fundamentais em causa[68].

5. Limites e restrições

Como se dá com os direitos fundamentais em geral, também o direito à proteção de dados pessoais está submetido a limites e admite (e mesmo exige) intervenções restritivas de diversa natura, sempre com o escopo – que opera como condição prévia de legitimação constitucional das restrições – de proteger outros direitos fundamentais ou bens jurídicos de estatura constitucional[69].

Quanto aos limites e restrições, toda e qualquer captação (levantamento), armazenamento, utilização e transmissão de dados pessoais, em princípio, constitui uma intervenção no âmbito de proteção do direito, que, portanto, como já adiantado, não prescinde de adequada justificação[70]. Outrossim, embora não se trate de direito absoluto, revela-se como um direito bastante sensível, tanto mais sensível quanto mais se tratar de dados pessoais sensíveis, associados a dimensões da dignidade da pessoa humana, implicando, de tal sorte, exigências mais rigorosas – e controle mais intenso – de eventuais intervenções restritivas[71].

No caso brasileiro, na condição de direito implicitamente positivado e enquanto não aprovada e promulgada emenda constitucional nos termos do projeto que ora tramita no Congresso Nacional (onde se faz expressa remissão à lei) não se cuida de direito

---

[68] Cf, por todos (porém com destaque para o ambiente da Internet) SCHLIESKY, Utz; HOFFMANN, Christian; LUCH, Anika D.; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. *Schutzpflichten und Drittwirkung im Internet.* Das Grundgesetz im digitalen Zeitalter. Baden-Baden: Nomos, 2014. p. 119 e ss.

[69] Cf., por todos, SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional, op. cit., 2018.

[70] Cf., por todos, WOLFF, Heinrich Amadeus. Schutz personenbezogener Daten. *In*: PECHSTEIN, Matthias; NOWAK, Carsten; HÄDE, Ulrich (Coord.). *Frankfurter Kommentar EUV – GRC – AEUV*. Tübingen: Mohr Siebeck, 2017. v. 1. p. 1117 e ss.

[71] Cf., por todos, STARCK, Christian. Art. 2 Abs. 1 – Schutz des Art. 2 Abs. 1 vor Eingriffen durch die öffentliche Gewalt. *In*: VON MANGOLDT; KLEIN; STARCK. *Grundgesetz Kommentar*, v. 1, 7. Auf. München: C.H.Beck, 2018. p. 217.

submetido (como no caso do sigilo das comunicações) a expressa reserva legal, mas a sua vinculação – ainda que não superposição integral – com os direitos à privacidade e intimidade sugere que se lhe dê proteção em princípio equivalente, como, aliás, defende a doutrina brasileira especializada.[72]

Nesse contexto, calha recordar que embora seja o direito à proteção de dados submetido a limites e passível de restrições, acionam-se, também nesse caso, os assim chamados limites aos limites dos direitos fundamentais, dentre os quais desponta a necessária observância dos critérios da proporcionalidade e da salvaguarda do núcleo essencial, o que se aplica seja qual for a origem e natureza da intervenção estatal (judiciária, administrativa e legislativa) na esfera de proteção do direito à proteção de dados.

Ainda nessa quadra, para efeitos do controle da legitimidade constitucional das restrições ao direito à proteção dos dados pessoais, assume relevo – como já adiantado! – a distinção entre dados considerados sensíveis, que dizem mais de perto com aspectos da vida íntima (dados sobre a orientação sexual, religiosa, a opção política, vida familiar, entre outros) e dados mais "distantes" desse núcleo mais sensível, como é o caso de informações sobre nome, filiação, endereço, CPF etc.[73]

Cuidando-se de dados relativos ao sigilo profissional, ou mesmo dados fiscais e bancários, importa levar em conta as diretrizes existentes para tais situações, submetidas, como direitos fundamentais autônomos, a um regime próprio, em que pese um conjunto de aspectos comuns.

Por outro lado, os limites e restrições ao direito à proteção de dados carecem de uma compreensão sistemática e que leve em conta simultaneamente sua dimensão subjetiva e objetiva, já que por conta dos deveres de proteção estatal de outros direitos, podem ser necessárias restrições à proteção de dados na perspectiva subjetiva, ou seja, intervenções no plano das posições jurídicas atribuídas aos titulares do direito.

Um exemplo extraído da jurisprudência do STF bem ilustra a situação. É o que se deu em relação ao embate entre direito de acesso a informações de caráter público e em poder de órgãos públicos (objeto de regulação, no Brasil, pela Lei 12.527/2011) e o direito à proteção de dados pessoais sensíveis (ligados à privacidade) dos servidores públicos. A conjugação do direito de acesso à informação com os princípios constitucionais da

[72] Cf. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, op. cit., 2019, p. 263-4.
[73] Cf, por todos, SAMPAIO, José Adércio Leite. A suprema inviolabilidade: a intimidade informática e o sigilo bancário, op. cit., p. 543.

publicidade e da transparência, levou o STF – embora não poucas as críticas endereçadas à decisão – a reconhecer que a proteção da privacidade dos servidores públicos é menor do que a do cidadão comum, de modo a considerar constitucionalmente legítima (proporcional) a divulgação nominal e individualizada dos seus vencimentos e benefícios[74].

Outros casos emblemáticos, como se dá com o assim chamado direito ao esquecimento, já lembrado acima, mas também conflitos entre a proteção de dados e liberdades comunicativas em geral, remetem a problemas como o da posição preferencial da liberdade de expressão e de quais são os critérios aptos a viabilizar um equacionamento mais consistente, do ponto de vista jurídico-constitucional, do problema[75].

Note-se, ainda, que a própria LGPDB prevê restrições de diversa natureza e para diversos efeitos, o mesmo se verificando em outros diplomas legislativos que já se encontram em vigor, como é o caso das já referidas Lei de Acesso à Informação e Lei do Marco Civil da Internet, restrições, aliás, que, em alguns casos, suscitam dúvidas e mesmo apresentam fortes indícios de serem constitucionalmente ilegítimas, aspecto que, todavia, aqui não temos condições de desenvolver, visto extrapolar o propósito do presente texto.

6. Considerações finais

Como se pode verificar ao longo do trabalho, venha – ou não – ocorrer a inserção de um direito à proteção de dados pessoais no texto da CF, a condição de direito fundamental autônomo não depende, em si, de tal expediente, porquanto sobejamente demonstrado que se trata de um direito implicitamente positivado, o que é objeto de amplo consenso doutrinário e mesmo acolhido na esfera jurisprudencial.

Seja na forma prevista no PEC 17, seja com outra formatação, é também correta a ponderação de que mediante a sua incorporação ao catálogo constitucional de direitos, um direito fundamental à proteção de dados pessoais daria maior sustentação ao marco regulatório infraconstitucional, bem como a sua aplicação pelos órgãos do poder judiciário, dentre outras vantagens apontadas.

Particularmente relevante é o fato de que a condição de direito fundamental vem acompanhada de um conjunto de prerrogativas traduzidas por um regime jurídico

[74] Cf. julgamento na SS 3.902, rel. Min. Teori Zavascki, j. 23.04.2015.
[75] Sobre o tema, v., entre outros, HARTMANN, Ivar. Liberdade de expressão e capacidade comunicativa: um novo critério para resolver conflitos entre direitos fundamentais informacionais, in: *Direitos Fundamentais & Justiça*, ano 12, n. 39, p. 145-183, jul./dez. 2018.

reforçado e uma dogmática sofisticada, mas que deve ser, em especial no caso brasileiro, desenvolvida e traduzida numa práxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação da proteção de dados com outros direitos e garantias fundamentais e bens jurídicos e interesses de estatura constitucional.

Nesse contexto, nunca é demais lembrar que levar à sério a proteção de dados pessoais é sempre também render homenagem à dignidade da pessoa humana, ao livre desenvolvimento da personalidade e à liberdade pessoal como autodeterminação.

7. Referências bibliográficas

ALEXY, Robert. *Theorie der Grundrechte*. 2. ed. Frankfurt a.M. Suhrkamp, 1994.

ANDRADE, Fábio Siebeneichler de. Notas sobre a aplicabilidade dos direitos da personalidade à pessoa jurídica como evolução da dogmática civil. *RJLB*, a. 4, n. 5, p. 806-837, 2018.

ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. Coimbra: Almedina, 1987.

BILBAO UBILLOS, Juan Maria. *Los derechos fundamentales en la frontera entre lo público y lo privado.* La noción de "state action" en la jurisprudencia norteamericana. Madrid: McGraw-Hill, 1997.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019.

BULL, Hans-Peter. *Informationelle Selbstbestimmung* – Vision oder Illusion?. Tübingen: Mohr Siebeck, 2009.

CANARIS, Claus-Wilhelm. Considerações a respeito da posição de proibições de discriminação no Sistema de Direito Privado. *Revista Direitos Fundamentais e Justiça*, a. 7, n. 22, jan./mar. 2013.

CANARIS, Claus-Wilhelm. *Grundrechte und Privatrecht.* Berlin-New York: Walter de Gruyter, 1999.

CONSELHO DA EUROPA. *Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais*, de 28 de janeiro de 1981. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 15 nov. 2019.

DIMOULIS, Dimitri; MARTINS, Leonardo. *Teoria Geral dos Direitos Fundamentais*. São Paulo: RT, 2007.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba, *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 15 nov. 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

DREIER, Horst. Art. 2 I – allgemeines Persönlichkeitsrecht. *In*: DREIER, Horst (Coord.). *Grundgesetz Kommentar*. 3. Auf. Tübingen: Mohr Siebeck, 2013.

DREIER, Horst. Subjektiv-rechtliche und objektiv-rechtliche Grundrechtsgehalte. *JURA*, 1994.

DUQUE, Marcelo Schenk. *Direito Privado e Constituição.* Drittwirkung dos Direitos Fundamentais. Sâo Paulo: Revista dos Tribunais, 2013.

FACHIN, Luiz Edson; RUZYK, Carlos Eduardo Pianovski. Direitos fundamentais, dignidade da pessoa humana e o novo código civil: uma análise crítica. *In*: SARLET, Ingo Wolfgang (Coord.). *Constituição, direitos fundamentais e direito privado*. Porto Alegre: Livraria do Advogado, 2003.

GOMES CANOTILHO, José Joaquim; MOREIRA, Vital. *Constituição da República Portuguesa anotada*, 4. ed. Coimbra: Coimbra Editora, 2007.

GOMES CANOTILHO, José Joaquim. Omissões normativas e deveres de proteção. *In*: DIAS, Jorge de Figueiredo (Coord.). *Estudos em homenagem a Cunha Rodrigues* Coimbra: Coimbra Editora, 2001. v. II.

GRIMM, Dieter. A função protetiva do Estado. *In*: SOUZA NETO, C. P.; SARMENTO, D. *A Constitucionalização do Direito*. Rio de Janeiro: Lumen Juris, 2007.

HARTMANN, Ivar. Liberdade de expressão e capacidade comunicativa: um novo critério para resolver conflitos entre direitos fundamentais informacionais. *Direitos Fundamentais & Justiça*, a. 12, n. 39, p. 145-183, jul./dez. 2018.

HESSE, Konrad. *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*. 20. ed. Heidelberg: C. F. Müller, 1995.

HILGENDORF, Eric; FELDLE, Jochen (Ed.). *Digitalization and the Law*. Baden-Baden: Nomos, 2018.

HOFFMANN, Christian; LUCH, Anika; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. *Die digitale Dimension der Grundrechte.* Das Grundgesetz im digitalen Zeitalter. Baden-Baden: Nomos, 2015.

HOFMANN-RIEM, Wolfgang. Reclaim Autonomy: Die Macht digitaler Konzerne. *In*: AUGSTEIN, Jakob (Coord.). *Reclaim Autonomy. Selbstermächtigung in der digitalen Weltordnung*. Frankfurt am Main: Suhrkamp, 2017.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The populational census decision and the right to informational self-determination. *Computer Law & Security Report*, v. 25, i. 1, 2009.

IPSEN, Jörn. *Staatsrecht II – Grundrechte*. 17. Auf. Vahlen, 2014.

JARASS, Hans; PIEROTH, Bodo. *Grundgezetz fur die Bundesrepublik Deutschland*: Kommentar. München: C. H. Beck. 13. Auf. 2014.

KARG, Moritz. Artikel 4, Nr. 1. *In*: SIMITIS, Spiros; HORNUNG, SPIECKER GENANNT DÖHMANN, Indra. *Datenschutzgesetz*. Baden-Baden: Nomos, 2019.

KLOEPFER, Michael. *Verfassungsrecht II*. München: C. H. Beck. 13. Auf. 2010.

KÜHLING, Jürgen. Datenschutz und die Rolle des Rechts. *In*: STIFTUNG FÜR DATENSCHUTZ (Ed). *Die Zukunft der informationellen Selbstbestimmung*. Berlin: Erich Schmidt Verlag, 2016.

LEONARDI, Marcel. *Fundamentos de Direito Digital*. São Paulo: Revista dos Tribunais, 2019.

LIMBERGER, Têmis. *O Direito à Intimidade na Era da Informática*. Porto Alegre: Livraria do Advogado, 2007.

MANSSEN, Gerrit. *Staatsrecht I Grundrechtsdogmatik*. München: Verlag Franz Vahlen, 1995.

MARINONI, Luiz Guilherme. *Técnica processual e tutela dos direitos*. 4. ed. São Paulo: Revista dos Tribunais, 2013.

MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. *Revista Direitos Fundamentais & Justiça*, a. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor. São Paulo: Saraiva, 2013.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): O Novo Paradigma da Proteção de Dados. *Revista de Direito do Consumidor*, v. 120, nov./dez. 2018.

MIRANDA, Jorge; MEDEIROS, Rui. *Constituição Portuguesa Anotada*. 1. ed. Coimbra: Coimbra Editora, 2006.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. *Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data*. Direitos Fundamentais & Justiça, a. 13, n. 41, p. 183-212, jul./dez. 2019.

MOTA PINTO, Paulo. *Direitos de Personalidade e Direitos Fundamentais*: Estudos, Coimbra: Gestlegal, 2018.

MURSWIEK, Dietrich; RIXEN, Stephan. Persönliche Freiheitsrechte. *In:* SACHS, Michael. *Grundgesetz Kommentar*. 8. ed. München: C.H.Beck, 2018.

PARLAMENTO EUROPEU. *Carta de Direitos Fundamentais da União Europeia*, de 7 de dezembro de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 15 nov. 2019.

PIEROTH, Bodo; SCHLINK, Bernhard. *Grundrechte*. Staatsrecht II. 11. ed. Heidelberg: C. F. Müller, 1995.

REINHARDT, Jörn. Conflitos de direitos fundamentais entre atores privados: "efeitos horizontais indiretos" e pressupostos de proteção de direitos fundamentais. *Direitos Fundamentais & Justiça*, ano 13, n. 41, p. 59-91, jul./dez. 2019.

RODRIGUES JÚNIOR, Otávio Luís. *Direito Civil Contemporâneo*: Estatuto Epistemológico, Constituição e Direitos Fundamentais. 2. ed. São Paulo: GEN, 2019.

ROSSNAGEL, Alexander; WEDDE, Peter; HAMMER, Volker; PORDESCH, Ulrich. *Digitalisierung der Grundrechte?* Zur Verfassungsverträglichkeit der Informations-und Kommunikationstechnik. Opladen: Westdeutscher Verlag, 1990.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. *Direito, Estado Sociedade*, n. 36, jan/jun. 2010.

RUFFERT, Matthias. Privatrechtswirkung der Grundrechte. Von Lüth zum Stadionverbot – und darüber hinaus?. n. 1, Jus 2020.

SAMPAIO, José Adércio Leite. A suprema inviolabilidade: a intimidade informática e o sigilo bancário. *In*: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coord.). *Direitos fundamentais no Supremo Tribunal Federal*: balanço e crítica, Rio de Janeiro: Lumen Juris, 2011.

SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. Direitos Fundamentais e Direito Privado, algumas considerações em torno da vinculação dos particulares aos direitos fundamentais. *In*: SARLET, Ingo Wolfgang (Coord.). *A Constituição Concretizada: Construindo Pontes para o Público e o Privado*. Porto Alegre: Livraria do Advogado, 2000.

SARLET, Ingo Wolfgang. Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988, Direitos Fundamentais & Justiça | Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. *O Direito ao "Esquecimento" na Sociedade de Informação*. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. 3. ed. São Paulo: Revista dos Tribunais, 2014.

SARMENTO, Daniel. *Direitos Fundamentais e Relações Privadas*. Rio de janeiro: Lumen Juris, 2003.

SCHIEDERMAIR, Stephanie. Einleitung. *In*: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GENANNT DÖHMANN, Indra (Coord.). *Datenschutzrecht*. Baden-Baden: Nomos, 2019.

SCHLIESKY, Utz; HOFFMANN, Christian; LUCH, Anika D.; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. *Schutzpflichten und Drittwirkung im Internet.* Das Grundgesetz im digitalen Zeitalter. Baden-Baden: Nomos, 2014.

SILVA, Virgílio Afonso da. *A Constitucionalização do Direito.* Os direitos fundamentais nas relações entre particulares. São Paulo: Malheiros, 2005.

SPIECKER GENANNT DÖHMANN, Indra. Kontexte der Demokratie: Parteien, Medien und Sozialstrukturen (1. Referat). *VVDStRL*. Berlin: De Gruyter, 2018.

_____O direito à proteção de dados na internet em casos de colisão, in: *Revista Direitos Fundamentais & Justiça*, a. 12, n. 38, p. 17-33, jan./jun. 2018.

STARCK, Christian. Art. 2 Abs. 1 – Schutz des Art. 2 Abs. 1 vor Eingriffen durch die öffentliche Gewalt. *In*: VON MANGOLDT; KLEIN; STARCK. *Grundgesetz Kommentar*, v. 1, 7. Auf. München: C.H.Beck, 2018.

STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais*. São Paulo: Malheiros, 2004.
STERN, Klaus. Idee und Elemente eines Systems der Grundrechte. *In:* KIRCHHOF, J. Isensee-P. (Coord.). *Handbuch des Staatsrechts der Bundesrepublik Deutschland*. Heidelberg: C. F. Müller, 1992. v. 5.

WOLFF, Heinrich Amadeus. Schutz personenbezogener Daten. *In*: PECHSTEIN, Matthias; NOWAK, Carsten; HÄDE, Ulrich (Coord.). *Frankfurter Kommentar EUV – GRC – AEUV*. Tübingen: Mohr Siebeck, 2017. v. 1.

A Protecção de Dados Pessoais em Angola: realidade, desafios e perspectivas

Amaro Santos Figueiredo[76]

RESUMO

Este artigo tem como objectivo apresentar considerações sobre o estado actual da protecção dos dados pessoais em Angola. Com efeito, analisa o quadro jurídico sobre a protecção de dados pessoais, o posicionamento da Agência de Protecção de Dados, enquanto entidade reguladora, faz uma descrição sobre a realidade, os desafios e os caminhos a percorrer para consolidação da protecção de dados pessoais em Angola. A principal conclusão a que se chegou é a de que a protecção de dados pessoais, em Angola, é um assunto "novo", pouco conhecido pela maioria dos cidadãos e instituições, sendo, por isso, enormes os desafios a enfrentar. A entrada em funcionamento da Agência de Protecção de Dados, em 2019, é vista como início de uma nova era, para a efectivação da protecção de dados pessoais, e espelha, finalmente, o engajamento do Estado angolano para com o assunto. Todavia, para melhor actuação, a Agência de Protecção de Dados deve ser transformada numa autoridade administrativa independente.

PALAVRAS-CHAVE

Angola; Protecção de dados pessoais; Agência de Protecção de Dados; Desafios; Perspectivas.

ABSTRACT

This article aims at presenting considerations on the current state of personal data protection in Angola. In effect, it analyzes the legal framework on the personal data protection, the positioning of the Data Protection Agency, as a regulatory body. Similarly, it describes the reality, challenges and paths to be taken to consolidate the personal data protection in Angola.

The main conclusion reached is that the personal data protection, in Angola, is a "new" subject, little known by most citizens and institutions, and therefore the challenges to be faced are enormous. The entry into operation of the Data Protection Agency in 2019 is seen as the beginning of a new era, for the realization of the personal data protection, and finally it reflects the engagement of the Angolan State in this matter. However, for better performance, the Data Protection Agency must be transformed into an independent administrative authority.

KEYWORDS

Angola; Personal Data Protection; Data Protection Agency; Challenges; Perspectives.

[76] Licenciado em Direito pela Universidade Agostinho Neto; Consultor e quadro sénior da Administração Pública há 14 anos, exerce atualmente a função de Administrador Executivo da Agência de Proteção de Dados da República de Angola. Professor colaborador do Instituto Superior de Ciências Sociais e Relações Internacionais (2008 a 2015). Tem formação especializada em: (i) Direito da Proteção de Dados - Universidade Automática de Lisboa (ii) Modernização da Legislação na Administração Pública e Promoção do Diálogo Social- Centro de Estudos da Organização Mundial do Trabalho em Itália (iii) Criminalidade Complexa e Técnicas de Investigação Criminal- Instituto de Estudos Judiciários.

Introdução

O progresso registado no sector das tecnologias de informação e comunicação, nas últimas décadas, muito se deve ao tratamento de dados pessoais. Se é verdade, por um lado, que a utilização destes dados proporciona inovação e qualidade aos produtos e serviços fornecidos aos cidadãos, também não é menos verdade que, a excessiva concentração de dados pessoais nas mãos dos poderes públicos e de particulares, em dimensões nunca antes vistas *(Big Data),* faz elevar o risco de intrusão à privacidade de cada indivíduo.

As nossas relações com a família, amigos, empresas e Administração Pública se concretizam, hoje, na maioria das vezes, através do mundo digital. Talvez, por isso mesmo, não fosse desprovido de sentido dizer que, vivemos subjugados e dependentes dos meios electrónicos, sendo certo que o problema, que aqui se levanta, é o da dimensão moral e ética destes meios e, fundamentalmente, quando confrontados com a questão da utilização de dados pessoais.

Tal como refere Franklim Foer (2018), "Dados" é um termo inócuo, mas aquilo que ele representa é de uma relevância ímpar. É o registo de acções: o que lemos, aquilo que assistimos, por onde andamos ao longo de um dia, a nossa correspondência, as nossas pesquisas, os pensamentos que começamos a digitar e depois apagamos.

Questões como colecta, acesso, partilha, manipulação, conservação e protecção dos dados revestem-se de uma de séria preocupação, uma vez que podem, de facto, colocar em causa a intimidade das pessoas. Por isso, é fundamental assegurar um justo equilíbrio entre a privacidade dos cidadãos e o progresso económico e social que se procura alcançar, tornando-se forçosa, neste sentido, a regulação do tratamento de dados pessoais.

Segundo Mafalda Barbosa (2017. p, 14) "Não se estranha por isso que, um pouco por todo lado, tenham surgido diversos diplomas tendentes a disciplinar a matéria. As preocupações que se começaram a sentir na década setenta do século XX determinaram, de facto, que em diversos ordenamentos jurídicos, fossem aprovadas as primeiras leis sobre protecção de dados".

Em Angola, a abordagem pública sobre a protecção de dados pessoais é um assunto que só agora começa a sair - ainda que timidamente - da sombra, graças à massificação das tecnologias de comunicação e informação, que o país vem conhecendo, associada à explosão do famigerado fenómeno das "redes sociais", cujo consumo desenfreado, a dado passo, começara a revelar-se potencialmente perigoso à privacidade

dos cidadãos e, não menos importante, a crescente onda de delitos cibernéticos, como o roubo de identidade, fraudes bancárias, pornografia infantil, crimes contra honra e outros. Com a presente abordagem, pretende-se trazer à estampa, ainda que, sumariamente, o quadro actual da protecção de dados em Angola, fazendo, de resto, uma incursão sobre o quadro legislativo de referência, a configuração da autoridade reguladora, os desafios actuais e os possíveis trilhos para a consolidação da protecção de dados pessoais.

1. O regime jurídico da protecção de dados em Angola

A protecção legal dos dados pessoais é matéria de criação recente, pois, foi com a actual Constituição da República de Angola (doravante CRA), aprovada em 2010, que se consagrou expressamente o direito à reserva da intimidade da vida pessoal e familiar [77] (cf. Artigo 32.º) e a providência do habeas data (cfr. artigo 69.º).

Na sequência da aprovação da CRA, e no quadro da reforma legal do sector das tecnologias de informação e comunicação encetada, pelo então Executivo, foi aprovada a Lei n.º 22/11, de 11 de junho, Lei da Protecção de Dados Pessoais (doravante LPDP).
Esta lei, conforme afirma Manuel Masseno (2020), aproxima-se à lei portuguesa na estrutura, nos conceitos e na própria redacção. Em traços gerais, o diploma contempla: os conceitos operatórios sobre protecção de dados pessoais; os princípios e requisitos que regulam o tratamento destes dados pessoais; a comunicação e transferência internacional de dados; os direitos dos titulares dos dados; as medidas de segurança a adoptar no tratamento de dados; as formalidades para comunicação ou autorização de tratamento; os requisitos específicos para o tratamento de dados nos sectores público e privado; a natureza e composição da Agência de Protecção de Dados e o regime sancionatório.

Em 2011, foi, igualmente, aprovada a Lei n.º 23/11 de 20 de Junho, Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação. Esta lei, para o que releva em matéria de protecção de dados pessoais, consagra: a protecção da privacidade e os direitos dos utilizadores de internet e outros meios de comunicação electrónica; as condições gerais de tratamento desses dados; as medidas técnicas e organizativas a que estão sujeitos os operadores e afirma a competência da APD,

[77] J.J Gomes CANOTILHO, & Moreira VIDAL. *Constituição da República Portuguesa Anotada*, Volume I, Coimbra Editora 4ª edição, 2007. pag.467 e 468: O direito à reserva da intimidade da vida privada familiar analisa-se principalmente em dois direitos menores: a) o direito a impedir o acesso de estranhos a informação sobre a vida privada e familiar e b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada de outrem.

enquanto entidade responsável pela fiscalização e aplicação do regime sancionatório, decorrente da violação destas normas (crf. artigos 14.º, 15.º 55.º, 60.º e 73.º).

Atendendo à necessidade de promover a inclusão digital, e fortalecer a utilização do espaço cibernético angolano, foi aprovada, em 2017, a Lei nº 7/17 de 16 de Fevereiro- Lei de Protecção das Redes e Sistemas Informáticos. O diploma em apreço, para além de definir as medidas de protecção do ciberespaço acessíveis ao público, consagra um conjunto de medidas de protecção de dados, de tráfego e de localização aplicáveis a operadores de comunicações electrónicas acessíveis ao público; as regras específicas aplicáveis aos prestadores de armazenagem principal, enquanto entidades tendencialmente mais vulneráveis a ciberataques; o regime sancionatório aplicável à violação das disposições da sobredita lei, cuja aplicação é, de igual modo, conferida à APD.

No plano continental, Angola ratifico, em 2019, a Convenção da União Africana sobre Cibersegurança e Protecção dos Dados Pessoais de 2014, por via da Resolução n.º 33/19, de 09 de Julho. Esta Convenção integra o compromisso dos Estados-membros da União Africana, de definir os objectivos e orientações gerais da Sociedade da Informação e fortalecer a legislação existente nos diferentes países.

No caso específico da protecção de dados, a Convenção preconiza um quadro jurídico comum sobre: direitos dos titulares dos dados; obrigações dos responsáveis pelo tratamento dos dados; repressão às infracções à privacidade; fluxos internacionais de dados e criação de autoridade nacional, de protecção de dados, assente em pressupostos de autonomia e independência.

Finalmente, e de grande alcance, realça-se a Declaração Universal dos Direitos do Homem, o Pacto Internacional dos Direitos Civis e Políticos e a Carta Africana dos Direitos do Homem e dos Povos, instrumentos ratificados por Angola e que reconhecem a necessidade de protecção e reserva à intimidade da vida privada.

1.1. A Agência de Protecção de Dados

Nos dizeres do n.º 1 do artigo 44.º da LPDP, a Agência de Protecção de Dados (APD), é uma pessoa colectiva de direito público, dotada de personalidade jurídica, com autonomia administrativa financeira e patrimonial. A APD é composta por sete membros, designados nos seguintes termos: três pelo Presidente da República, dos quais nomeia o Presidente da Agência; três eleitos pela Assembleia Nacional; um Magistrado Judicial eleito Conselho Superior da Magistratura Judicial, (cfr. nº 2 do artigo 44º da LPDP).

A APD funciona na dependência do Titular do Poder Executivo e rege-se pela LPDP, pelo seu Estatuto Orgânico, aprovado pelo Decreto Presidencial nº 214/16, de 10 de Outubro, pelo regime dos institutos públicos e demais legislação em vigor do funcionalismo público.

As atribuições da APD vêm prescritas no artigo 44º LPDP. Porém, esta lista de atribuições é complementada pelo artigo 5.º do Decreto Presidencial nº 214/16, de 10 de Outubro.

Com efeito, compete à APD o seguinte:

a) Fiscalizar a aplicação das disposições da LPDP;
b) Emitir recomendações, orientações e instruções sobre as melhores práticas no tratamento de dados pessoais;
c) Emitir parecer sobre o acesso aos documentos nominativos.
d) Emitir parecer sobre o sistema de classificação de documentos;
e) Apreciar e decidir sobre as reclamações que sejam dirigidas à APD e garantir o exercício do direito de acesso, de rectificação, actualização e eliminação de dados pessoais;
f) Registar e publicar o registo de ficheiros de dados pessoais;
g) Garantir aos titulares dos dados pessoais a obtenção de informação precisa sobre os seus direitos no âmbito do tratamento dos seus dados;
h) Orientar a aplicação das medidas técnicas e de seguranças necessárias e adequadas;
i) Cooperar com as autoridades internacionais em matéria de protecção de dados pessoais e fiscalizar os movimentos internacionais de dados pessoais;
j) Exercer a sua função sancionatória em matéria de protecção de dados pessoais, nos termos da lei de protecção de dados pessoais.
k) Inspeccionar e fiscalizar o tratamento automatizado e não automatizado dos dados pessoais e respectivos ficheiros;
l) Emitir parecer sobre a aplicação da lei de protecção de dados pessoais e demais actos complementares.

Do catálogo de atribuições supracitado, pode-se inferir que o legislador confiou à ADP três tipos de poderes, designadamente: poderes de consulta e autorização; poderes de investigação; e poderes de sanção.

Uma das questões centrais, que se suscita em torno da configuração jurídica da APD, tem que ver com o facto de não possuir atributos de uma verdadeira entidade administrativa autónoma e independente, como é comum suceder com as autoridades de protecção de dados contemporâneas.

Para Carlos Morais (2000.p, 103) "Podemos caracterizar autoridade administrativa independente, em sentido lato, como toda a instância de natureza pública criada pela Constituição ou pela lei tendo em vista o exercício predominante da função administrativa, em que, para esse efeito, o mesmo centro de poder ou seus membros se

encontrem sujeitos a vínculos de subordinação a qualquer órgão jurídico-público, ou a interesses organizados que respeitem ao domínio sobre o qual incide a sua atividade".

No caso concreto da APD, a falta de independência é questionada não só pelo facto de a mesma ser uma entidade superintendida[78], mas também por inexistir um regime de imunidades e incompatibilidade para os seus membros.

De acordo com António Cordeiro, (2020. p, 402) "A independência é alcançada, *grosso modo,* vedando qualquer influência, direta ou indireta que possa condicionar o desempenho das funções e o exercício dos respetivos poderes".

Com efeito, infere-se dos artigos 12.º e 13.º do Decreto Presidencial n.º 214/16, de 10 de Outubro, que, o Conselho de Administração da APD pode ser dissolvido, por razões de reestruturação ou em consequência de mudança de orientação deste, quanto à respectiva gestão, sendo os respectivos membros exonerados a todo o tempo.

Francisco Coutinho (2020), argumenta que a garantia de independência destas entidades visa assegurar a eficácia e a confiança da fiscalização e observância do direito à protecção de dados, devendo ser compreendida à luz deste propósito.

Note-se, igualmente, que a independência das autoridades é um dos principais critérios usados para a avaliação do nivel de adequação da protecção de dados de qualquer Estado, sendo que, a ausência deste pressuposto pode impactar, por conseguinte, no livre fluxo transfronteiriço de dados pessoais. Por exemplo, o Regulamento Geral de Protecção de Dados da União Europeia (2016), é bastante elucidativo nesta matéria ao dispor na alínea b) do n.º 2 do artigo 45.º, que a Comissão, ao avaliar o nível de protecção, tem em conta, dentre outros aspectos, a existência e o real funcionamento de uma ou mais autoridades de controlo independente no país terceiro.

A Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais exige, conforme referenciado atrás, que cada Estado-parte crie uma autoridade de protecção de dados independente e autónoma. Por isso, Angola, enquanto parte signatária, está obrigada a harmonizar e ajustar o modelo organizacional e funcional da APD ao preceituado no artigo 11.º da sobredita Convenção, por forma a torná-la numa verdadeira autoridade administrativa autónoma e independente.

[78]António Francisco de SOUSA. Manual de Direito Administrativo Angolano. Edição Vida Económica – Editorial, SA, 2014. pág., 109. A superintendência consiste no poder que um ente de fins múltiplos tem de estabelecer os fins e orientar a acção de um ente dele auxiliar ou dependente. O poder de orientação da superintendência assinada uma maior intensidade destes poderes relativamente aos poderes de controle da tutela administrativa, não se confundido também com os poderes de direcção, típicos da hierarquia administrativa.

2. As perspectivas e desafios

Apesar de a APD ter sido institucionalizada formalmente em 2011, pela LPDP e o respectivo modo de organização e funcionamento, aprovado em 2016, entretanto, o seu efectivo funcionamento só veio a ocorrer em Outubro de 2019[79], após designação do seu primeiro Conselho de Administração.

Como se pode inferir, a APD é uma instituição nova, cujo percurso foi afectado, no seu primeiro ano de existência pela pandemia da Covid-19. Atento ao catálogo de deveres cometidos à APD, julgamos serem desafios e prioridades a prosseguir as seguintes:

2.1.Organizar e fortalecer a capacidade interna.

Estando a APD numa fase embrionária, deve a mesma ser suficientemente dotada de recursos humanos, financeiros e matérias para a prossecução das suas missões.

Sabe-se que o capital humano é o coração de qualquer organização, por isso mesmo impõe-se que a APD tenha quadros com conhecimento técnico especializado. Isso significa deter um número suficiente de juristas, profissionais da segurança da informação, tecnologistas, economistas e outros com especialidade técnica importante, levando em consideração as características e a dimensão do país.

Recorde-se que, esta necessidade está suficientemente vincada na Convenção da União Africana sobre Cibercrime e Protecção de Dados Pessoais que, insta os Estados-parte a adoptarem as autoridades de protecção de recursos humanos, técnicos e financeiros necessários para o cumprimento da sua missão[80].

2.2. Fomentar a cultura de protecção de dados pessoais entre os cidadãos e as organizações.

Com aproximadamente nove anos de vigência, a LPDP é o principal diploma legal sobre protecção de dados pessoais em Angola, entretanto, os cidadãos e as organizações pouco ou nada sabem sobre ele. Esta realidade, marcadamente preocupante nos dias de hoje, obriga a que sejam rapidamente gizadas estratégias para a educação dos cidadãos a volta dos seus direitos e deveres. De igual modo, às organizaçõesdevem ser treinadas e esclarecidas sobre as suas obrigações e responsabilidades, quanto ao tratamento dos dados pessoais.

[79]Data da tomada de posse do seu Conselho de Administração, nomeado pelo Decreto Presidencial nº 277/19, de 06 de Setembro.

[80] Cfr. nº 8º do artigo 11º.

A promoção de fóruns (o plural correcto de fórum é fora por causa do latim) de discussão, junto das instituições de ensino e das associações profissionais; a criação de um repositório de informação, física e electrónica, de acesso público; a publicação regular de boletins informativos e a difusão de publicidade institucional, parecem revelar-se ferramentas de grande utilidade para o alcance de tal desiderato.

Por isso, a APD, enquanto ente director da protecção de dados, tem de assumir, neste processo, uma posição de vanguarda na educação, consciencialização e orientação de todas as partes envolvidas, por via de um plano de comunicação claro e perspicaz.

2.3. Elaborar directrizes de conformidade.

Atendendo ao facto de as instituições públicas e privadas não disporem ainda (substituir por já) de um nível de maturidade assinalável, quanto ao tratamento de dados, e sendo certo que existem áreas da LPDP que exigem esclarecimento adicional, a APD tem a responsabilidade de elaborar regras, procedimentos e linhas orientadoras com vista a auxiliar as organizações na correcta interpretação e aplicação da lei *(frameworks de conformidade*).

Instituições do sector privado, como a banca, seguros, telecomunicações, ensino, saúde e grandes retalhistas, bem como a Administração Pública no geral, devem merecer uma especial atenção face à sensibilidade e ao volume de dados que processam.

Neste interím, é crível, por exemplo, serem emitidos notas orientadoras sobre o tratamento de dados no contexto da saúde; no contexto laboral; no contexto da realização de campanhas e marketing político; sobre padrões técnicos e organizacionais relativos à segurança de dados, etc.

2.4. Dinamizar a componente inspectiva

O sucesso e a capacidade de afirmação da APD, perante os responsáveis pelo tratamento de dados, está indubitavelmente atrelada à sua capacidade de fiscalizar, supervisionar e fazer cumprir as disposições legais e regulamentares sobre protecção de dados.

Para tal, a APD deve estar munida de recursos e desenvolver competências que lhe permitam realizar auditorias aos suportes informáticos que contenham dados.

2.5.Operacionalizar a cooperação internacional e a transferência de dados pessoais

No âmbito das suas atribuições, à APD compete assegurar a representação do Estado angolano, junto de organismos e eventos internacionais sobre protecção de dados, bem como dinamizar acções e intercâmbio neste domínio.

Sendo a APD uma instituição recente, reveste-se de prioridade estratégica a sua filiação nos principias organismos, regionais e internacionais, que congregam as autoridades de protecção, assim como promover a celebração de acordos de cooperação para o fortalecimento das suas capacidades.

A transferência internacional de dados é uma componente fundamental da actividade da APD, pois cabe a ela verificar e definir em que circunstância uma organização pode transferir dados pessoais para fora das fronteiras do Estado.

Sendo um dos domínios vitais para a dinamização do ambiente de negócios, é imprescindível que a APD conheça os procedimentos técnicos internacionais para a certificação de transferência.

2.6.Apoiar a transformação digital da economia Angolana

No âmbito do Plano Nacional de Desenvolvimento (o actual é Plano de Desenvolvimento Nacional) (2018-2022)[81], o governo angolano definiu, de entre as acções prioritárias, a promoção, apoio e dinamização da cultura de inovação e empreendedorismo tecnológico.

A ADP tem de se assumir como peça fundamental nessa transformação digital, definindo padrões técnicos para proteger os dados pessoais[82] de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, modificação, comunicação ou qualquer forma de tratamento inadequado.

3. Conclusão

No decorrer desse estudo, observa-se que Angola, está numa fase embrionária, em matéria de protecção de dados pessoais, e tem pela frente uma longa trajectória.

---

[81] Ver o *Plano de Desenvolvimento Nacional de Angola (2018-2022)*. Disponível em: https://www.ucm.minfin.gov.ao/cs/groups/public/documents/document/zmlu/njax/~edisp/minfin601408.pdf

[82]Bruno Ricardo BIONI. Proteção de Dados Pessoais. A Função e os Limites do Consentimento. Edição – Editora Forense LTDA, Brasil, 2020. pág, 176.: "Se, por um lado, a tecnologia pode ser invasiva à privacidade informacional, como se verificou no caso dos trackers. Por outro lado, ela pode ser uma ferramenta para proteção dos dados pessoais, tal como propõem as denominadas *Privcy Enhancing Technologies*/PETs".

A instituição da APD, em 2019, numa altura que Angola se encontrava (ainda se encontra) mergulhada numa profunda crise económica, evidencia o interesse das autoridades em tornar efectiva a protecção da privacidade e dos dados pessoais dos cidadãos.

Para a concretização desse objectivo, aponta-se como urgente, tornar a APD numa verdadeira entidade administrativa autónoma e independente, com recursos humanos, financeiros e técnicos para a prossecução das suas missões, impondo-se, ainda, o envolvimento dos cidadãos e das instituições para a promoção de uma cultura de protecção de dados, bem como a inserção da APD nos organismos internacionais, que congregam as autoridades de protecção de dados.

A existência de uma autoridade de protecção de dados forte trará reflexos positivos para a melhoria da imagem externa do país, em matéria de respeito e consolidação dos direitos, liberdades e garantias fundamentais dos cidadãos. Poderá, igualmente, contribuir para a melhoria do ambiente de negócios e para o alavancar do sector das tecnologias de comunicação e informação do país.

4. Referências bibliográficas

Livros

CANOTILHO, Jorge J Gomes & VITAL, Moreira (2007). Constituição da República Portuguesa Anotada, Volume I. Edição - Coimbra Editora 4ª edição.

BARRETO, A. Menezes Cordeiro (2020). Direito da Proteção de Dados à Luz do RGPD e da Lei Nº 58/2019. Edição - Edições Almedina, Coimbra.

BIONI, Bruno Ricardo (2020). Proteção de Dados Pessoais. A Função e os Limites do Consentimento. Edição – Editora Forense LTDA, Brasil.

FOER, Franklim (2018). Mundo Sem Mestre, A Ameaça Existencial da Alta Tecnologia. Edição -Temas e Debates – Circuito de Leitores, Lisboa.

SOUSA, António Francisco de (2014). Manuel de Direito Administrativo Angolano. Edição. Vida Económica, Editorial, SA

Capítulo de Livro e Revista

BARBOSA, Mafalda Miranda (2017). Proteção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os Benefícios da Proteção e a Responsabilidade Civil. In Revista do Instituto do Conhecimento AB. Ano V. Nº 7. Porto-Portugal.

COUTINHO, Francisco Pereira (2020). A Independência da Comissão Nacional de Proteção de Dados. In (COUTINHO, Francisco Pereira & MONIZ Graça Canto(coord). Anuário da Proteção de Dados. Edição – Universidade Nova de Lisboa. Faculdade de Direito, Lisboa, Portugal.

Legislação
Constituição da República de Angola, de 5 de Fevereiro de 2010. Publicação em Diário da República de Angola, Série I, N.º 23. Disponível em: http://www.parlamento.ao/c/document_library/get_file?uuid=0bdfe610-1be4-48a0-a1f5-bfdc7f497d7d&groupId=243313

Resolução nº 33/19, de 09 de Julho, pela Assembleia Nacional, que aprova a Convenção da União Africana sobre Cibersegurança e Protecção dos Dados Pessoais de 2014. Disponível em: https://www.lexlink.eu/legislacao/geral/14793/ia-serie/por-tipo-de-documentolegal/2019/91

Lei nº 22/11, de 17 de Junho, Lei da Protecção de Dados Pessoais. Publicação em Diário da República de Angola, Série I, N.º 114. Disponível em: https://media2.mofo.com/documents/Law_22_11_Data_Privacy_Law.pdf

Lei nº 23/11 de 20 de Junho, Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação. Publicação em Diário da República de Angola, Série I, N.º 130. Disponível em: https://www.inacom.gov.ao/fotos/frontend_6/editor2/decreto_presidencial_no_166_14-9_julho_de_2016-22_de_novembro_de_2017.pdf

Lei nº 7/17 de 16 de Fevereiro, Lei de Protecção das Redes e Sistemas Informáticos. Publicação em Diário da República de Angola, Série I, N.º 27. Disponível em: https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf

Decreto Presidencial nº 214/16, de 10 de Outubro, aprova o Estatuto Orgânico da Agência de Protecção de Dados. Publicação em Diário da República de Angola, Série I, N.º 171. Disponível em: https://www.minfin.gov.ao/cs/groups/public/documents/document/mjew/mjqu/~edisp/-128202969813101602 1024.pdf~1.pdf

Decreto Presidencial nº 277/19 de 6 de Setembro, que nomeia o Conselho de Administração da Agência de Protecção de Dados. Publicação em Diário da República de Angola, Série I. N.º 116. Disponível em: https://angolaforex.com/2019/09/13/diario-da-republica-i-a-serie-n-o-116-de-6-de-setembro-de-2019/

Outras Fontes da Internet
MASSENO, Manuel David (2018). A Proteção de Dados Pessoais em Portugal e nos outros Países de Língua Portuguesa, uma cartografia das Fontes Legislativas. Disponível em http://direitoeti.com.br/artigos/a-protecao-de-dados-pessoais-em-portugal-e-nos-outros-paises-de-lingua-portuguesa-uma-cartografia-das-fontes-legislativas/ . Acesso,10/12/2020.

MORAIS, Carlos Blanco (2000). As Autoridades Administrativas Independente na Ordem Jurídica Portuguesa. Disponível em https://portal.oa.pt/upl/%7B5a323e37-4297-4bd2-97d5-7ccb97a3a31d%7D.pdf . Acesso, 08/01/2021.

Plano Nacional de Desenvolvimento de Angola (2018-2022). Vol. I. Disponível em https://www.ucm.minfin.gov.ao/cs/groups/public/documents/document/zmlu/njax/~edisp/minfin601408.pdf . Acesso, 10/01/2021.

Regulamento da Parlamento Europeu e do Conselho 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, de 27 de Abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679Acesso, 18/12/2020.

Da proteção de dados a uma política pública de privacidade

Maria Cláudia Cachapuz[83]
Maria Luiza Kurban Jobim[84]

RESUMO

Este artigo propõe a discussão sobre autodeterminação informativa, em face das atividades específicas de armazenamento, registro e transmissão de dados. Propõe o debate quanto à reciprocidade de conduta na esfera pública relativamente ao ato de conhecer o que há de informação sobre o indivíduo e como se manifesta o tratamento da informação pela gestão dos bancos de dados nominativos. O artigo ainda se preocupa em debater o conceito de autodeterminação informativa e como se dispõe um direito geral de liberdade à possibilidade do exercício de sua restrição. No texto, além da apreciação sobre os princípios orientadores de um direito de acesso, há o debate sobre a implementação de uma política de privacidade junto às instituições públicas e a experiência específica de implementação da LGPD no âmbito do Tribunal de Justiça do RS/ Brasil.

PALAVRAS-CHAVE

autodeterminação informativa, proteção de dados, privacidade, política pública, Poder Judiciário.

[83] Doutora em Direito pela Universidade Federal do RS (UFRGS)/Brasil. Professora de Direito Privado da UFRGS. Magistrada do Tribunal de Justiça do RS e membro da Comissão para Implantação da LGPD no TJRS.
[84] Mestre em Direito pela Universidade de Kent (Reino Unido). Assessora jurídica do Tribunal de Justiça do RS e membro da Comissão para Implantação da LGPD no TJRS.

From data protection to a public privacy policy

ABSTRACT

This article deals with the informational self-determination discussion, in regard to the specific activities of storage, registry and data transfer. It entails the debate about reciprocity of conduct in the public sphere related to the acknowledgment of personal information stored in public databases and how its respective management is presented. The article is concerned with the conceptualization of the informational self-determination and aims at understanding how the general right to freedom embraces respective possibilities in terms of constraints. Besides the analysis of the guiding principles surrounding the right to access, there is the debate surrounding the implementation of a privacy policy alongside public institutions and the specific case analysis of the LGPD implementation in the Tribunal de Justiça do RS/Brazil. (...)

KEYWORDS

information self-determination, data protection, privacy, public policy, Judiciary.

Introdução

Muito já se passou desde o dia em que João Carlos Gabrois conheceu o pai, militante político, por fotografia, pela primeira vez, aos 19 anos de idade. O encontro ocorreu em meio a várias pastas de documentos, numa sala da Secretaria de Cultura do Estado de São Paulo, em março de 1992. A foto de André Gabrois, integrante do Partido Comunista do Brasil e morto no incidente conhecido como Guerrilha do Araguaia, em 1973, era apenas uma entre as centenas espalhadas na mesa. Como muitos outros familiares de desaparecidos, João Carlos, à época, apenas revelava o desejo de saber onde se encontravam os restos mortais do pai, para proporcionar-lhe "um sepultamento normal, desses que todas as famílias fazem"[85].

Desde a época do relato oferecido pela família Gabrois até o período mais recente de plena vigência da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709, de 14.08.2018) no Brasil, é significativo o avanço do estudo nas questões relacionadas à publicização de informações privadas por parte do poder público, incluindo a necessidade de elaboração de normatividade suficiente para se enfrentar o tema do silêncio em relação a informações apontadas como de segurança nacional. Em que pese se possa hoje reconhecer relativa superação do episódio inicialmente narrado – inclusive pelo pagamento de indenizações pelos ilícitos reconhecidos no passado político brasileiro e pela publicação de uma normativa ampla em relação ao acesso de informações públicas (Lei nº 12.527, de 18.11.2011) -, muito há ainda que ser feito em relação à interpretação da normatividade positivada, de forma a garantir-se efetividade e correta aplicação aos enunciados dogmáticos editados. Principalmente, quando se trata de compatibilizar a Lei nº 12.527/11 (Lei de Acesso à Informação) à efetiva implementação de uma política de proteção de dados no âmbito das instituições públicas brasileiras. Saber compatibilizar o interesse público de transparência de informações com o interesse privado de sigilo de dados pessoais parece se traduzir no desafio contemporâneo da gestão pública. Nada muito diferente do alerta efetuado por Hannah Arendt, ainda na década de 1970, em pleno século XX: "A busca imprudente dos interesses privados na esfera pública-política é tão desastrosa para o bem público quanto

[85] Relato reproduzido em trecho da reportagem "Uma luz no porão", de autoria de Antônio Carlos Padro e Luís Fernando Sá, publicada na Revista Isto É/Senhor, nº 1173, de 25.03.1992. Sobre a matéria restou elaborado parcial estudo sobre a matéria no texto "Informática e proteção de dados: Os freios necessários à automação", publicado na Revista da Ajuris, AJURIS, Porto Alegre, nº 70, ainda no ano de 1997, p. 374-409.

são as tentativas arrogantes dos governos de regular a vida privada de seus cidadãos para a felicidade privada" (ARENDT, 1977, p. 104).

Isto se dá porque no cerne da LGPD brasileira está a preocupação explícita (art. 2º, inc. II) com um conceito de *autodeterminação informativa*, em que pressuposta a necessidade de compreensão de uma situação jurídica corriqueiramente levada à apreciação dos tribunais: o enfrentamento da proteção da privacidade quando em discussão o registro, o armazenamento e a transmissão de dados pessoais coletados no âmbito de instituições públicas. Ou seja, há que se conhecer em que medida é possível realizar-se o registro e a manutenção de dados nominativos em bancos cadastrais públicos – assim como se espera o mesmo cuidado em relação aos bancos cadastrais privados -, enfrentando-se os princípios pertinentes à matéria e indagando-se quanto ao acesso, ao tempo de esquecimento, à extensão da transmissão de dados a terceiros.

Essa ação e reação sistemática ao avanço da ciência, especialmente em áreas de maior desenvolvimento tecnológico, revela a tendência do cidadão contemporâneo de aprender a lidar com a sua individualidade sem necessariamente abdicar de um benefício tecnológico que lhe facilita o contato com uma esfera pública de relacionamento. Ou mesmo que lhe garanta, de forma ampla, no âmbito do poder público, a participação nas questões de Estado e, portanto, de efetivo exercício da cidadania. Veja-se que, ainda na década de 1990, Paul Virilio mencionava o exemplo de uma pessoa que, "para lutar contra os fantasmas que pareciam persegui-la" (VIRILIO, 1999, p. 61), instalara câmeras de vídeo na residência, permitindo que os visitantes de seu espaço de divulgação na Internet pudessem auxiliá-la no combate a eventuais fantasmas que a assombravam, num exercício não muito diferente daquele usufruído por quem hoje explora, com certa facilidade, a própria imagem em espaços destinados a efetivos diários de confissão pública, como o *Instagram* e o *Facebook*.

Poder-se-ia, portanto, questionar em que medida a esfera pública - ou aquilo que a represente no mundo das aparências (ARENDT, 1993) – tem se traduzido em espaço de reflexão ao indivíduo - na essência, resguardado ao privado -, ou mesmo até que ponto se pode reconhecer uma nova concepção de liberdade para o desenvolvimento (livre) da personalidade na sociedade contemporânea. E justamente porque se reconhece que o compartilhamento de dados ocorre de uma forma muito mais complexa na contemporaneidade, justamente em razão dos avanços tecnológicos na adoção de elaboradas ferramentas de cruzamento de dados. Uma realidade que, mesmo nas perspectivas mais sombrias de Hannah Arendt – de que "o governo que não é nem da

lei, nem dos homens, mas dos escritórios ou computadores autônomos, cuja dominação inteiramente despersonalizada pode vir a se tornar uma ameaça maior à liberdade e àquele mínimo de civilidade sem o qual nenhuma vida comunitária é concebível, do que jamais foi a mais abusiva arbitrariedade dos tiranos do passado"(ARENDT, 2004, p. 66) -, não se imaginaria aceita de forma tão automática e natural, como simples consequência da evolução cultural e tecnológica da humanidade.

O tema, de fato, não é mais novidade em termos jurídicos. Ainda em sentença datada de 15 de dezembro de 1983[86], o Tribunal Constitucional Federal da Alemanha, ao analisar a extensão de questionamento possível ao cidadão por meio de uma legislação censitária, reconheceu a oportunidade de autodeterminação informativa a todo indivíduo, de forma que toda e qualquer informação pessoal só se tornasse pública *se* justificada por um determinado interesse público e *se* conhecida do titular tanto a sua existência como a extensão de seu compartilhamento. Ainda assim, a liberdade de autorização individual ao que se faz divulgado permite restrições, considerando o Tribunal Constitucional da Alemanha que "a autodeterminação é uma condição elementar de funcionamento de uma comunidade democrática fundada sobre capacidade de agir conjuntamente de seus cidadãos. [...] A informação, ainda quando relacionada a pessoa, apresenta uma figuração da realidade social, a qual não pode ser exclusivamente subordinada ao afetado"[87].

Ao afirmar, expressamente, uma liberdade individual de controle da própria informação – ainda que esta não se encontre insuscetível de restrição -, o Tribunal Constitucional observou, abstratamente, uma exigência de reciprocidade de conduta[88] na esfera pública, para conhecer e tornar conhecido o que é, por uma primeira definição, íntimo e privado ao cidadão. Possibilitou que se compatibilizassem prerrogativas relacionadas a um direito geral de liberdade, reconhecendo-se tanto o livre arbítrio ao indivíduo - e, assim, a possibilidade de discutir uma vontade no âmbito público -, como a proteção ao que é de sua essência – aquilo que lhe é exclusivo. Portanto, reconhece que o sigilo só é justificado quando em benefício do próprio indivíduo, e não quando se torna uma ferramenta ao controle de sua liberdade individual. Daí a possibilidade de se

[86] BVerfGE 65,1.
[87] BVerfGE 65,1, em tradução livre da versão alemã.
[88] Tércio Sampaio Ferraz Júnior, citando Wolfgang Hoffmann-Riem, esclarece que o que denomina como "autodeterminação informacional" não é um "direito de defesa privatístico do indivíduo que se põe à parte da sociedade, mas objetiva possibilitar a cada um uma participação em processos de comunicações" (FERRAZ JR., 2001, p. 242).

"garantizar la esfera personal estricta de la vida y la conservación de sus condiciones básicas" (ALEXY, 2001, p. 356), sem que se abdique de uma concepção igualmente ampla de liberdade ao indivíduo e, mais especificamente, de livre desenvolvimento de sua personalidade.

A concepção de autodeterminação informativa, nos termos como acolhida pelo tribunal alemão, autorizou, por primeiro, a adoção de um critério de objetivação da vontade em relação à conduta de tornar público aquilo que pertence, com exclusividade e reserva, ao indivíduo, permitindo, a partir de mecanismos de controle, que a informação seja partilhada no âmbito público, desde que suficientemente justificado esse compartilhamento e atribuída a respectiva responsabilidade a que efetue o tratamento dos dados. Em outras palavras, a sentença de 1983, na Alemanha, pôs em relevo, pela primeira vez, o papel e a extensão do consentimento individual junto aos bancos cadastrais públicos, discutindo a relação entre autodeterminação informativa e transparência de dados estatísticos a partir de uma perspectiva de proporcionalidade no exame do tema[89].

1. Proteção de dados e autodeterminação informativa

Em relação ao tratamento dispensado à proteção de dados nominativos[90], matéria que desafia a comunidade jurídica contemporânea relativamente à questão da privacidade, o conceito de autodeterminação informativa tem igualmente contribuído para orientar a atividade do intérprete, ao reconhecer a autonomia do indivíduo tanto dirigida ao controle e à transmissão de informações personalíssimas como encaminhada à possibilidade de acesso à qualquer informação. Tal qual acentuava Agostinho Eiras, à

[89] Como anota Jürgen Schwabe, na discussão da decisão alemã, "hasta donde obligan el derecho a la autodeterminación de la información y el principio de la proporcionalidad relacionado con éste, así como la obligación del legislador a reglamentar de oficio mediante disposiciones constitucionales estas reglas, depende de la clase, extensión y posible utilización de los datos recolectados, así como del peligro de su abuso" (SCHWABE, 2003, p. 40).

[90] Consideram-se dados nominativos, de forma mais ampla, aquelas informações relativas às pessoas físicas identificadas ou identificáveis - no caso, uma identificação direta ou indireta, que possa ser promovida a partir dos dados que se apresentam processados separadamente ou conjuntamente. Há, para parte da doutrina, aceitação de que o termo "dados nominativos" seja utilizado da mesma forma que "dados pessoais" ou "dados de caráter pessoal", ainda que para abranger a totalidade dos dados relacionados à pessoa. Os dados nominativos devem corresponder a informações capazes de permitir uma identificação de seus titulares. Ou seja, capazes de criar uma relação de associação a uma pessoa determinada ou determinável em concreto, autorizando, em contrapartida, uma garantia protetiva à sua intimidade e vida privada. Conferir o histórico da discussão específica sobre a matéria em ORTIZ, 2002, p. 139.
A LGPD brasileira optou de forma expressa a utilizar as expressões "dado pessoal" e "dado pessoal sensível", com definições bem específicas (art. 5º, inc. I e II), diferenciando-as da expressão "dado anonimizado" (art. 5º, inc. III).

luz da experiência portuguesa, de forma pioneira no exame da matéria, "são objectivos fundamentais das normas sobre protecção de dados a transparência dos actos de administração, a reserva da vida privada e a garantia dos direitos do homem. As informações fichadas pelas autoridades públicas e privadas devem ser transparentes" (EIRAS, 1992, p. 68).

Fundamental para identificar uma efetiva proteção aos dados pessoais dos indivíduos numa sociedade informatizada é de que o controle sobre o armazenamento e a transmissão de dados possa ser realizado pelo titular da informação. Ou seja, é imprescindível ao titular de dados de que exerça a supervisão sobre a informação que lhe compete tanto em relação (i) à demonstração conferida por um interesse público no armazenamento de dados, como (ii) à justificação de uma transmissão do conteúdo informativo a terceiros, reconhecida sempre a possibilidade de interferência do indivíduo neste processo de acesso e correção de dados.

Isto se vê reconhecido, num primeiro momento, a partir do estabelecimento – inclusive legislativo[91] – de um amplo direito de acesso dos indivíduos às suas informações nominativas[92]. O próprio armazenamento de dados pessoais está informado por um princípio de acesso amplo aos titulares das informações, seja para o

[91]Identifica-se uma tendência de edição e aprimoramento de leis específicas sobre a matéria, especialmente em países integrantes da Comunidade Europeia, após a divulgação da Diretiva 95/46/EC. Uma preocupação que, em países da Europa e da América do Norte já se revelava, na década de 1970, existente ainda quando preponderante uma atividade de armazenamento manual de dados – no caso, principalmente dos chamados "dados sensíveis", através de fichários não-informatizados. No Brasil, a preocupação no estabelecimento de garantias especiais à proteção de dados pessoais se fez refletida, inicialmente, nas relações de consumo, passando a Lei 8.078/90 a disciplinar a atuação dos bancos cadastrais ligados à atividade específica de consumo. Posteriormente, dispôs a Lei 12.527/11 sobre tratamento da informação, com enfoque específico na garantia do direito de acesso às informações armazenadas em bancos públicos e privados de dados, garantindo a preservação a dados pessoais exclusivamente no art. 31 da referida norma. Tal não afastou a possibilidade de se examinar a matéria, de forma mais ampla, a partir do espectro das relações civis, e não, de forma pontual, das relações específicas de consumo. A disciplina conferida pelo art. 21 do Código Civil de 2002 ofereceu exame mais amplo que se pretende a matéria, regrando abrangentemente a proteção das questões relacionadas à privacidade e à intimidade. A Lei 8.078/90, na medida em que reservada às relações de consumo, passa, portanto, a complementar o ordenamento jurídico civil, preocupando-se com o problema da autodeterminação informativa no espaço de relacionamento em que, de forma especial e mais corriqueiramente, as situações de ameaça à intimidade e à vida privada se manifestam a partir da divulgação de informações pessoais. A matéria hoje é atendida, de forma específica, no art. 2º, inc. II, da LGPD.

[92] No âmbito constitucional, restou considerada inovadora a criação de um remédio constitucional como o *habeas data*, ainda no texto original da Constituição Federal (art. 5º, inc. LXXII), destinado a possibilitar o acesso e a retificação de informações a qualquer pessoa. Na prática jurisprudencial, a previsão constitucional tem se traduzido antes como um norte jurídico – de prerrogativa constitucional relativa ao acesso a informações nominativas -, do que propriamente como um efetivo instrumento de uso forense para a defesa de interesses privados. Nos tribunais, a defesa do direito de acesso tem sido postulada, com frequência, por meio de tutelas inibitórias mais amplas, que abranjam, cumulativamente, a possibilidade indenizatória em face de prejuízo demonstrado em concreto – situação inatingível por meio de um remédio constitucional.

reconhecimento de existência do próprio registro, seja para a verificação da extensão, veracidade e correção das informações armazenadas. Por isso, ressalta-se a relevância de uma previsão normativa específica, como inicialmente existente na Lei 8.078/90 (Código de Defesa do Consumidor), impondo a comunicação de registro de dados pessoais do consumidor em cadastro de consumo e crédito. No caso de formação de banco cadastral para o qual não fornece o indivíduo pessoalmente o conteúdo informativo – quanto mais, referindo-se, em regra, ao armazenamento de dados desfavoráveis a seus integrantes pela constatação de uma situação de inadimplência no mercado de consumo (art. 43, parágrafos 4º e 5º da Lei 8.078/90) ou pelo oferecimento de reclamações contra fornecedores de produtos e serviços (art. 44) -, essencial é o titular da informação ter, desde logo – e, portanto, desde o momento do armazenamento de uma informação -, ciência de que integra uma listagem informativa. E tal listagem pode, até mesmo, conter informações que lhe sejam, pelos efeitos gerados, desfavoráveis.

A matéria restou abrangida na LGPD por meio da ideia de que o direito de acesso deva facilitar o conhecimento acerca das informações sobre o tratamento dos dados. Portanto, não se trata, unicamente, de reconhecer a existência do tratamento e a sua finalidade, mas identificar que a disponibilidade das informações ao titular dos dados se dê "de forma clara, adequada e ostensiva" (art. 9º da LGPD) desde sempre. Daí porque se permite reconhecer, junto ao texto normativo brasileiro que se o direito de acesso é marcado, inicialmente, por um princípio de conhecimento acerca do armazenamento de dados, é pelo princípio da transparência ou da publicidade[93] que atinge a realização plena de um conceito de autodeterminação informativa[94]. É que não basta saber sobre a existência de um registro de informações pessoais, se, em concreto, não é fornecida ao titular das informações a possibilidade de fiscalização do conteúdo existente em registro.

De fato, ainda que tolerável a formação de bancos de dados com informações negativas em relação ao seu titular – porque considerada relevante a proteção das relações de crédito sob um princípio de lealdade contratual entre os integrantes de um mercado de negócios e de consumo -, não se concebe que essas informações ignorem a realidade factual mais verídica possível, guardada a mesma tônica de confiança –

[93] Esclarece Ana Ortiz, com enfoque à experiência espanhola de disciplina sobre a proteção de dados pessoais geridos por bancos cadastrais: "Sin la proclamación del principio de publicidad los derechos de los ciudadanos se resentirían y padecerían una grave quiebra en su efectividad y satisfacción" (ORTIZ, 1998, p. 247).

[94] Agostinho Eiras chega a afirmar que um direito mais concreto à autodeterminação informativa se desdobra em outros tantos direitos que visam assegurar a atuação do indivíduo frente a seu patrimônio informativo. Assim, em EIRAS, 1992, p. 78.

abstratamente considerada – exigida aos relacionamentos privados. Por isso a necessidade para o indivíduo, como garantia de um amplo direito de acesso às informações pessoais armazenadas em bancos cadastrais, de que não só ele tenha conhecimento quanto à existência de inscrição em banco de dados, como tenha ainda a possibilidade de alterar o conteúdo de um registro não correspondente à realidade descrita, independentemente da sua natureza – se de crédito, de consumo, de associação (ideológica, política, religiosa, cultural). Assim, é também resultante de um amplo direito de acesso o exame da medida de extensão do registro de informações pessoais efetuado. Mais precisamente, aborda-se aqui não apenas a possibilidade de uma restrição sobre o conteúdo informativo, como também a hipótese de pertinência do registro sobre determinado interesse público, pela qualidade da informação. A ideia de qualidade da informação aparece, via de regra, como uma das condições de sustentação e proteção de uma esfera de privacidade[95], quando analisados modernos sistemas de interconexão de dados pessoais por bancos cadastrais.

Rememorando a origem histórica e tomando como exemplo a normativa norte-americana sobre a matéria, encontra-se, ainda no Privacy Act de 1974, a preocupação de que as agências de coleta e armazenamento de dados retenham apenas aquelas informações que se tornem relevantes e que justifiquem o próprio cadastramento[96]. Mesma preocupação evidenciou-se na política pública de controle da privacidade, especificamente em relação às agências norte-americanas de armazenamento de dados no setor privado. Entre os princípios de privacidade estabelecidos a partir do programa de Information Infrastructure Task Force, editado ainda em 1995 pelo governo federal, encontrava-se já, entre os princípios, o reconhecimento à promoção de "qualidade à informação". Ou seja, a informação pessoal deve ser "exata, atual, completa e relevante

[95] Assim explica Ana Isabel Ortiz: "La 'calidad de los datos' como principio sobre el que se asienta la licitud de la recogida y del tratamiento posterior de los mismos ha de contemplarse desde una doble perspectiva: la 'cualidad del dato personal' y la finalidad del tratamiento. Por tanto, los datos alcanzan determinada calidad y es lícito su tratamiento porque son puestos en relación con los fines legítimos que inspiran el tratamiento. Luego, el dato será adecuado cuando se encuentre directamente relacionado con la finalidad concreta, cuando sea necesario para el cumplimiento de la misma; pero, por otro lado, también será adecuado cuando responda a la veracidad y exactitud e integridad de la información relativa a la persona, y finalmente, el dato no será excesivo cuando sea proporcionado respecto a dicha finalidad, esto es, que sean los datos estrictamente necesarios para su cumplimiento, y su recopilación no sea abusiva ni desproporcionada en relación con la finalidad de cada tratamiento" (ORTIZ, 2002, p. 211).

[96] Ainda na origem, pelo Privacy Act, as agências de controle de bancos cadastrais ligadas ao setor público deveriam atender os seguintes princípios: "(1) armazenar apenas informação pessoal que seja relevante e necesaria; (2) coletar o máximo de informação possível sobre determinado assunto; (3) manter arquivos de forma completa e atual; (4) estabelecer mecanismos administrativos e técnicos de segurança sobre os registros" (CATE, Fred H., 1997, p. 77).

para as finalidades que justificam sua coleta e utilização"[97]. Nada diferente do que reconhece, mais recentemente, o artigo 9º da LGPD brasileira.

Algo, inclusive, que restou acolhido ainda no momento de edição da Lei de Acesso à Informação no Brasil. Mesmo havendo a possibilidade de previsão de informações de caráter sigiloso - porque submetidas temporariamente à restrição de acesso público em razão da imprescindibilidade para a segurança da sociedade e do Estado -, preocupou-se a normatividade em estabelecer graus e prazos de sigilo, sem que se possa vetar a possibilidade de discussão do interessado quanto ao acesso, inclusive por meio de recurso administrativo quando necessário, cabendo à instituição pública necessariamente indicar a autoridade competente ao exame da matéria. Ou seja, mesmo quando sigilosa a informação, não se descarta a necessidade de que a autoridade pública justifique a negativa de acesso, qualificando o interesse público mais relevante e graduando a concessão da informação na medida de sua disponibilidade pública de acesso.

A qualidade da informação importa ainda no reconhecimento de um princípio com atuação simultânea, e não menos relevante, relacionado ao tempo de registro das informações pessoais. Fala-se, por isso, no princípio do esquecimento[98], orientado pela compreensão de que o próprio gestor do banco cadastral se compromete a manter atualizados os registros, fiscalizando o tempo de sua permanência em face da finalidade que o determina[99]. Não por outra razão, disciplinava, ainda na sua origem, a Diretiva

---

[97] Tal se deduz da tradução livre à regulamentação de um princípio de "qualidade da informação" (item n. 6 do capítulo de princípios e comentários da Information Infrastructure Task Force).

[98] Como antes já havia anotado, "a disciplina decorre da compreensão de que informações desfavoráveis sobre determinada pessoa não podem permanecer armazenadas em caráter perpétuo, a ponto de prejudicarem outras relações de convívio da pessoa atingida – principalmente relações de consumo -, tendo em vista dados antigos, até mesmo coletados de forma equivocada e sobre os quais não foi exercitado o direito de retificação. A Lei brasileira de Defesa do Consumidor, neste ponto, é específica, prevendo duração máxima de cinco anos para as informações negativas cadastradas em bancos de dados sobre consumo" (CACHAPUZ, 1997, p. 389).

[99] No Brasil, muito se discutiu, inicialmente, sobre a melhor interpretação a ser conferida ao tempo de registro previsto aos bancos cadastrais de consumo, em face da previsão legislativa constante no parágrafo 1º do art. 43 da Lei 8.078/90. Tal discussão é anterior ao debate proposto junto ao STJ quanto à aplicação de um direito ao esquecimento com reflexos no âmbito da responsabilidade civil independentemente do reconhecimento de um tempo específico para fins prescricionais quanto ao registro da informação. A discussão inicial tomou relevo quando o Superior Tribunal de Justiça firmou jurisprudência no sentido de que "nenhum dado negativo persistirá em bancos de dados e cadastros de consumidores por prazo superior a cinco anos. Tratando-se, entretanto, de dívida não paga, não se fornecerá a seu respeito informação, pelos sistemas de proteção de crédito, de que possa resultar dificuldade de acesso ao crédito, se, em prazo menor, verificar-se a prescrição". A solução para dívidas que tinham a possibilidade de prescrição da ação em tempo inferior a cinco anos encaminhou-se no sentido de promoção de uma suspensão ao ato de tornar pública a informação - salvo em hipótese suficientemente justificada que não se fizesse estritamente relacionada à mora do devedor e, por certo, a partir de uma ponderação promovida no nível dos princípios -, ainda que o cancelamento definitivo do registro só ocorra posteriormente. Em caráter excepcional,

95/46/EC, de 24 de outubro de 1995, destinada aos países membros da Comunidade Europeia, em seu artigo 6º, alínea 'e', que o registro de um dado pessoal deve ser armazenado de tal forma que possibilitasse a identificação da própria relevância de sua manutenção. Vê-se a obrigação, inclusive, de que fossem promovidas formas de resguardo das informações que tenham de ser registradas por um longo período, em razão de sua importância histórica, estatística ou científica. O que, de forma mais específica, restou mantido pelo 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, especialmente no capítulo III, ao tratar do direito à limitação de tratamento pelo titular dos dados. Algo vinculado, desde sempre, à finalidade prevista para o tratamento adotado[100].

Também se encontra relacionada a um direito mais amplo de acesso às informações nominativas do indivíduo - que se vejam registradas em banco cadastral - a

contudo, reconheceu o STJ, na oportunidade, a possibilidade de prescrição em tempo inferior ao de cinco anos quando a matéria discutida escapasse da seara de consumo. Assim, em hipótese de ação indenizatória por danos extrapatrimoniais, relativa à inscrição indevida de nome em órgão de restrição de crédito promovida por banco e atinente a negócio jurídico bancário. No caso, restou aplicada a prescrição prevista no § 3º do art. 206 do Código Civil brasileiro, "tendo em vista que a inscrição indevida decorre de um vício de adequação do serviço realizado pelo banco [...], não sendo caso de reparação de danos causados por fato do produto ou serviço, requisitos essenciais para a aplicação do prazo prescricional descrito no artigo 27 do CDC" (BRASIL. STJ. AgRg no Ag 1418421/RS. Relator: Min. Paulo de Tarso Vieira Sanseverino. Brasília, DJ de 13.08.2013).

[100] Assim o próprio parágrafo (39), estabelecendo os motivos de justificação ao texto normativo do Regulamento: "O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da 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. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas quando da recolha dos dados pessoais. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas."

característica essencial da veracidade do conteúdo informativo armazenado. Isto corresponde, em resumo, à ideia de que todo registro deve preservar uma nota de autenticidade em relação ao seu conteúdo, implicando a necessidade de que as informações armazenadas sejam não apenas precisas, como completas.

Ainda ao tempo da Diretiva Europeia, de outubro de 1995, ao arrolar os princípios que inauguravam a proteção específica à privacidade em relação ao processamento de dados nominativos, preocupou-se a normatividade europeia em conferir completude ao conceito de veracidade das informações registradas, permitindo, assim, o afastamento – pela retificação, pelo bloqueio ou pelo cancelamento - de toda e qualquer informação que não atinja esta característica de exatidão exigida[101]. Conforme a disciplina legislativa, "todo razoável esforço deve ser efetuado para assegurar que o dado que seja impreciso ou incompleto, considerado a partir da finalidade para a qual foi coletado e pela qual está sendo armazenado, seja apagado ou retificado"[102]. Situação não diferente da acolhida pelo Regulamento (UE) 2016/679, especialmente pelos arts. 5º (1), alínea 'd', e da norma.

Não há, então, como dissociar a compreensão de manutenção de um registro adequado, dada a veracidade de seu conteúdo, de uma garantia concomitante pelo direito à retificação, bloqueio ou cancelamento de informações que não correspondam, na sua integralidade, à realidade dos fatos espelhados. Situação que, na recente legislação nacional, restou amparada tanto pelos efeitos de ilicitude estabelecidos junto ao art. 32 da LAI, como, na essência, pela disciplina do art. 6º, inc. V, e art. 18 da LGPD brasileira.

Por fim, é relacionada à ideia de um direito amplo de acesso a informações nominativas registradas em bancos cadastrais a própria concepção de correção dos dados. Ou seja, não basta que o registro corresponda a uma situação factual, e, sim, que a informação esteja de acordo com o momento atual de registro, em especial, sobretudo, na hipótese de um parcial pagamento de dívida pelo consumidor, que imponha a atualização dos valores informados ao banco cadastral de relação de consumidores inadimplentes. A correção dos dados informativos é característica complementar à de veracidade das informações, remetendo também a uma possibilidade de retificação de conteúdo informativo quando evidenciado qualquer equívoco em concreto.

[101] Isto abrangia, inclusive, o direito do indivíduo a conhecer a lógica empregada para a compilação dos dados em determinado tipo de arquivo ou registro. Ver a redação do parágrafo 41 do preâmbulo da Diretiva 95/46/EC, de 24 de outubro de 1995.
[102] Neste sentido se encontra a disciplina da Diretiva 95/46/EC, de 24 de outubro de 1995, em seu art. 6º, n. 1, alínea 'd'.

Como a ideia de autodeterminação informativa apropria-se de conceitos relacionados tanto a um espaço de interferência marcante do direito de liberdade (esfera privada), como de interferência mais acentuada do direito de igualdade (esfera pública), identifica-se também num direito de acesso a dados informativos a possibilidade de o indivíduo ter acesso a informações que lhe sejam justificadamente importantes ou de revelação essencial. Abstratamente, a hipótese responde ao conceito de autodeterminação informativa como trabalhado pelo Tribunal Constitucional Federal da Alemanha, pois exige a reciprocidade de conduta a quem se dispõe à liberação dos dados e a quem pretende obter determinado acesso. Ou seja, permite-se, pelo exercício da ponderação, a partir da análise de situações concretas envolvendo direitos fundamentais, que dados nominativos sejam tornados públicos quando suficientemente evidenciada a sua relevância ao interessado. Isto ocorre porque mesmo interesse ideal de acesso atinge toda a coletividade. O exemplo trazido é o correspondente ao registro de dados históricos, estatísticos ou científicos que, por suas características peculiares, devam ter adequado acesso, útil e rápido, a qualquer indivíduo. E, no caso, estende-se o exemplo também aos dados nominativos relacionados a personalidades ou eventos com importância pública – porque considerados relevantes a uma esfera pública de convivência e determinantes de uma justificação científica[103].

Na recente experiência brasileira, evidencia-se este trabalho de garantia ao acesso de informações como objeto central de disciplina tanto na edição da Lei de Acesso à Informação (LAI) - inclusive preocupando-se a normatividade em oferecer, ainda *a priori,* como norte de interpretação (art. 31), a ponderação específica entre situações de reserva (privacidade) e de interesse público ao se tratar de informação pessoal, ainda que sempre sujeita eventual ameaça de lesão à apreciação judicial específica – quanto no

[103] É como constava ainda na Diretiva 95/46/EC, entre as justificativas apresentadas no parágrafo 29 para a regulação de uma proteção específica à transmissão de dados pessoais, em que acolhido previamente o interesse público de caráter histórico, científico ou estatístico para determinadas informações pessoais.Pertinente é a questão, portanto, em relação ao recente debate sobre as biografias não autorizadas. Para a resolução do conflito, imprescindível que, no tema, enfrente-se o problema da ponderação entre princípios e da possibilidade ampla de restrições a direitos fundamentais. No caso, por se tratar, ao fundo, quanto à discussão de um direito geral de liberdade, capaz de sofrer restrições quando sujeito a ponderações em relação ao caso concreto estabelecido no âmbito das relações entre privados. O que não colide, de forma alguma, com a proibição constitucional à censura, como disposta no art. 220 da Constituição Federal. Neste artigo, tem-se norma jurídica específica que tutela a relação do cidadão perante o Estado. Entre privados, a discussão jurídica a ser trabalhada é justamente a de ponderação, na análise de liberdades colidentes, a partir de princípios que alcançam, no valor abstrato, mesma preponderância jurídica. Assim, em relação aos princípios acolhidos nos incisos IV e X do art. 5º da Constituição Federal, a serem sujeitos a uma ponderação quando evidenciado o conflito pertinente a uma publicação não-autorizada entre privados. Para melhor elucidar o tema, tendo enfrentado especificamente o conflito: CACHAPUZ, 2006 e 2018, p. 173-191.

texto atual da LGPD brasileira, especialmente no trato dos bancos cadastrais públicos. O que permite, portanto, que se inclua a observação à ponderação – com possibilidade de restrição ao próprio consentimento, quando justificado – para fazer preceder o interesse público de acesso à informação em face do interesse particular do titular dos dados pessoais, como na hipótese de observância de um direito coletivo e público preponderante. Interpretação, por certo, que deve inspirar, na mesma medida, o sentido inverso de pretensão, quando precedentes condições fáticas e jurídicas que esbarrem em direitos fundamentais daqueles que tenham o interesse de acesso – e nessa medida justificado – a informações classificadas como sigilosas.

Espera-se, a partir da concepção de uma autonomia informativa, portanto, que haja uma reciprocidade ideal de comportamento na esfera pública de todos os que participem de um movimento de troca de informações. Primeiro, porque toda restrição à liberdade de transmissão de informações, apoiada em princípios de conhecimento, qualidade, esquecimento, veracidade e correção dos dados informativos, não interessa exclusivamente ao titular da informação, e, sim, a toda coletividade, para ter acesso aos dados armazenados. Segundo, porque a exigência de reciprocidade envolve tanto o interesse, puro e simples, de restrição de uma liberdade, como a promoção de uma conduta responsável a todo aquele que se dispõe, reciprocamente, a participar do espaço de troca de informações.

2. O estabelecimento de uma política pública de privacidade

A LGPD brasileira consolida, pois, as diversas dimensões – em fluxos informacionais complexos, transversais e simultâneos – observadas à autodeterminação informativa na era digital. Em um contexto cada vez maior de digitalização das interações institucionais e de *datificação* (MAYER-SCHÖNBERGER e CUKIER, 2014) a oportunidade de disposição sobre as informações que digam respeito ao titular de dados pessoais - e, portanto, o poder deste de se opor aos efeitos jurídicos a que restará sujeito -, emerge como regra geral, a partir da concretização efetiva do princípio da autodeterminação informativa. Ainda que muitos dos princípios e diretrizes gerais da LGPD pudessem ser extraídos de uma interpretação sistemática de comandos constitucionais sobre diplomas legais diversos[104], a sua contribuição reside em unificá-los e traduzi-los de forma concreta, para além de estabelecer deveres explícitos de forma ampla a todos aqueles

[104] Como exemplo podemos citar: o Código Civil, a LAI, o Marco Civil da Internet, o Código de Defesa do Consumidor, dentre outros.

envolvidos no tratamento de dados pessoais, inclusive àqueles investidos em ações de finalidade pública.

O desiderato é, nos dizeres da própria LGPD, art. 1º, *in fine*, dentre outros, a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural. Com destaque, encontra-se a própria ideia, no âmbito da esfera pública, do exercício pleno de *cidadania*[105] pelas pessoas (art. 2º, VII, *in fine*), conceito este estritamente relacionado ao entorno público que lhe é correlato. Na contemporaneidade, o conceito antes estático dos espaços e limites em que exercida a cidadania são substituídos por maior fluidez em um contexto ambivalente, pois à medida que permite ao cidadão adentrar facilmente em ambientes públicos acessíveis por meio de tecnologias diversas, obriga-lhe a *consentir*, em contrapartida, a uma maior exposição de sua vida privada. No presente contexto, é inexorável a relação umbilical da cidadania com o tratamento de dados pessoais no âmbito do setor público.

Nesse sentido, surge a LGPD brasileira com aplicação a ser observada, não apenas em relação a bancos cadastrais privados, mas igualmente por bancos de tratamentos de dados no âmbito do Poder Público. Trata-se de norma que congrega, pela generalidade que lhe é inerente, tanto aspectos tradicionalmente pertencentes ao ramo do Direito Público quanto do Direito Privado – nisso residindo, inclusive, a sua complexidade. O que permite, de certa forma, observar-se uma interação, no espaço digital, cada vez mais fluida entre os espaços destinados ao que é público e privado, tornando cada vez menos identificável a necessária distinção entre elas[106].

Em recente estudo realizado pela Organização para Cooperação e Desenvolvimento Econômico (OCDE, 2020), foi enfatizada a importância da cidadania digital como meio propulsor de maior eficiência na prestação de serviços governamentais. A participação facilitada nos canais de acesso no âmbito do poder público tem por escopo

[105] Seguindo uma interpretação sistêmica, conforme Kerber, na sua origem, a concepção aristotélica do termo cidadania é relacionada àquele que contribui para a elaboração ao mesmo tempo em que está também sujeito à observância das normas que regem determinada sociedade (KERBER, 1997). É a cidadania, aliás, que, para repelir o fim trágico previsto por Hannah Arendt no que toca à dominação dos "escritórios e dos computadores autônomos", garante o governo da lei *dos homens* para o exercício da liberdade essencial tanto contra o reino dos autômatos quanto àquele *mínimo de civilidade à vida comunitária* e basilar ao funcionamento de um Estado Democrático (ARENDT, 2004, p. 66). Quanto aos efeitos nefastos da falta civilidade e da limitação às liberdades, disserta Fromm, no âmbito da psique-social, o seu papel na insurreição de Estados totalitários. (FROMM, 1974).

[106] Sobre o ponto, Solove disserta sobre os desafios de conceituar privacidade no âmbito dos registros públicos dessa era da informação para além do preto-e-branco que associa privacidade com a esfera privada e o público com a transparência. (SOLOVE, 2004). Aqui, a ideia de proteção de dados parece trazer maior maleabilidade ao conceito, ainda que, nos Estados Unidos, este seja integrado uma das inúmeras faces do que se costuma chamar, simples e complexamente, de *privacidade*.

permitir maior aperfeiçoamento das políticas públicas baseadas em evidências, diminuindo os custos de transação respectivos a ambos os polos da relação (instituições e cidadão). Não é sem razão que, antes mesmo da LGPD brasileira, o Marco Civil da Internet (Lei nº 12.965/2014) já reconhecia que "o acesso à internet é essencial ao exercício da cidadania" (art. 7º, caput). Por outro lado, a facilitação criada pelos canais de comunicação computadorizados permite uma acessibilidade ampla não apenas do cidadão para com Estado, mas também deste para com aquele – em graus muito mais elevados e com um retrato muito mais elaborado. *De que* forma, *por que*, *para que* e *por quanto tempo* determinados dados pessoais serão tratados são, pois, questões igualmente relevantes.

No anseio de responder às aspirações de desburocratização e de modernização máquina pública, por meio do Decreto nº 10.046/2019, restou criado o Cadastro Base do Cidadão, visando à unificação dos dados de todas as pessoas, sob o argumento de maior eficiência e aprimoramento dos serviços públicos ofertados. No entanto, a sistemática adotada, ao correlacionar, de forma direta, *privacidade e sigilo* e *publicidade e acessibilidade irrestrita,* em relação aos dados pessoais compartilháveis entre as diversas unidades integrantes da esfera federal, tem gerado severas críticas por parte da sociedade civil. Recentemente, a Ordem dos Advogados do Brasil (OAB) inaugurou debate relevante[107], por meio de ação direta de inconstitucionalidade, apontado inconsistências na estruturação do Cadastro Base do Cidadão, especialmente quanto à relativa vagueza das normas estabelecidas, à ausência de clareza na especificação de um interesse público suficiente e a potencial desproporcionalidade no manuseio de dados pessoais entre as unidades governamentais. Dúvidas, portanto, permanecem quanto à possibilidade de interferência do Estado sobre a disposição de liberdades individuais, enquanto as instituições públicas, por dever legal decorrente da própria LGPD, começam a expedir atos administrativos para a disciplina de políticas de segurança de dados no âmbito da administração pública.

A LGPD brasileira entra, em sua maior parte, em vigor no ano de 2020: ano de pandemia pela COVID-19 e em que as atividades presenciais, tanto na esfera pública quanto na esfera privada, são majoritariamente substituídas pelas interações *on-line*,

[107] Processo n. 49.0000.2020.004727-9/Conselho Pleno Classe: Processo. Solicitação de propositura de Ação Direta de Inconstitucionalidade em face de dispositivos do Decreto n. 10.046/2019. Relator(a): Conselheiro Federal Rodolpho Casar Maia de Morais (RR).

exigindo, em face da política de distanciamento social, a confiança no estabelecimento da comunicação interpessoal por meio de plataformas digitais. A mudança drástica de comportamento, em certa medida, acelera a implantação da normatividade de segurança de dados, exigindo adaptações instantâneas, principalmente no âmbito público.

Um dos preceitos fundamentais da LGPD, ao se tratar da adequação normativa no âmbito do setor público, é compreender que *proteção* de dados pessoais *não é* – nem deve ser – sinônimo de *proibição*. Anteriormente já se defendeu (CACHAPUZ, 2018) que entre a configuração e a restrição de qualquer direito – e, especialmente, de direitos que tratem do exercício de liberdades -, deve ser levada em consideração a circunstância de que o caráter de razoabilidade ou mesmo de justiça acolhido para a edição de uma norma e para a tipificação de uma conduta (pelo estabelecimento de uma proibição, de um fazer obrigatório ou mesmo pelo estabelecimento de competências que atinjam o exercício de posições jurídico-civis), a partir do uso de argumentos jusfundamentais, não afasta a dimensão restritiva desta mesma norma, quando atinja um direito geral de liberdade ou de igualdade da pessoa (ALEXY, 2001, p. 324). A preocupação de Alexy, no ponto, é com o fato de que qualquer limitação de um direito fundamental possa ser interpretada, equivocadamente, como parte da determinação de seu conteúdo. Tal construção jurídica tornaria sempre necessário um condicionamento do exame de qualquer restrição à hipótese de abuso de um direito, porque pressuposto um determinado conteúdo conformador de um direito previamente pelo sistema jurídico. Por isso, há que se distinguir: uma realidade é a das normas de configuração de institutos de Direito Civil - gerando competências específicas para o caso de capacidade, casamento, propriedade, estabelecimento de sociedade -, em que há a confirmação de determinadas garantias constitucionais jusfundamentais. Nessas hipóteses, é possível que se vejam estabelecidas situações de conformação de direitos, para garantir-se, justamente, a titularidade de determinadas posições jurídicas. Outra circunstância é a das normas que, estabelecendo proibições ou determinações de um fazer específico – como no caso da harmonização necessária entre Lei de Acesso à Informação e LGPD -, gerem restrições ao exercício de liberdades. Ainda que sejam necessárias tais restrições, não se reconhece na liberdade residual – que é o produto da interpretação em abstrato pelo legislador – necessariamente a configuração de um direito, e sim, um produto justificado de uma ponderação. Não é, pois, o desiderato da LGPD proibir a existência de dados ou a extração de informações – até porque seria notoriamente ineficaz e ineficiente se o fizesse –, mas sim coordenar o

seu tratamento, oferecendo as condições fáticas e jurídicas de ponderação para toda e qualquer pretensão de ações de tratamento de dados pessoais.

Exemplificando por meio de estudo de caso, o Tribunal de Justiça do Rio Grande do Sul (TJRS) vem desenvolvendo, desde meados de 2020, sucessivas ações de forma a adequar-se à normativa nova de proteção de dados, atendendo ainda a orientações administrativas de regulação de conduta, em especial, a Recomendação nº 73/2020 do Conselho Nacional de Justiça (CNJ). Em maio de 2020, no âmbito administrativo da Corte, restou instaurado expediente administrativo próprio, visando à criação de um grupo trabalho para análise das medidas necessárias à adequação da instituição às diretrizes relacionadas à proteção de dados pessoais. Em momento subsequente, foi expedido ato que criou uma comissão de estudos específica para a implementação da LGPD no âmbito do TJRS (Ato nº 027/2020), publicando-se, na sequência, portarias de nomeação de seus respectivos membros (058, 068/2020 e 112/2020).

A partir de então, distintas ações de capacitação e formação foram delineadas e executadas para que houvesse um nivelamento técnico-jurídico no assunto aos membros da Comissão[108], permitindo-se o mapeamento dos principais setores envolvidos com o tratamento de dados pessoais na instituição. Parcerias com entidades de ensino foram realizadas para a capacitação do público interno no tema da proteção de dados[109] e diversas reestruturações, nos procedimentos humanos e informáticos, estão sendo conduzidas a fim de proporcionar maior clareza e transparência aos fluxos de dados pessoais no TJRS. Em outubro de 2020, o TJRS apontou, também, o seu encarregado da proteção de dados pessoais (Portaria nº 094/2020-P), para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Para interpretar-se e aplicar-se a LGPD no plano interno, bem como para pautar todas as demais ações e tarefas a serem executadas prospectivamente, o TJRS publicou o Ato nº 37/2020-P, datado de 18 de setembro de 2020 – mesma data de início de vigência da maior parte dos dispositivos da LGPD –, instituindo a sua política de proteção e segurança de dados pessoais[110].

[108] Nesse sentido, ocorreram as "Conversas sobre Proteção de Dados", nos dias 11, 14 e 24 de agosto de 2020, da Comissão para Implementação da LGPD no TJRS, com os professores Danilo Doneda, Márcia Fernandes e Maria Cristina Caldeira.
[109] Curso on-line "Os Desafios no Setor Público", realizado em parceria com o Instituto de Tecnologia e Sociedade (ITS), que se realizou do dia 24 ao dia 27 de novembro de 2020.
[110] Íntegra do ato disponível em: https://www.tjrs.jus.br/static/2020/09/Ato-037-2020-P-LGPD.pdf

O ato parte de cinco pontos fundamentais como pressupostos: (i) a harmonização da LGPD com a LAI; (ii) o estabelecimento de diretrizes gerais de proteção e segurança de dados; (iii) o controle amplo da informação; (iv) a disseminação da cultura de proteção de dados e a qualificação do método decisório humano frente às questões de informatização; e (v) o alinhamento da política de segurança de proteção de dados com ações de *compliance*. Ao longo de quinze dispositivos, a norma administrativa busca sintetizar a complexidade do tratamento de dados pessoais a ser dispensado no âmbito da instituição e, com isso, viabilizar o conhecimento prévio da matéria pelos agentes de tratamento junto ao público em geral.

Tal política não é realizada sem a constatação da omnipresença dos dados pessoais na sociedade informativa, capaz de permitir o aperfeiçoamento da operabilidade da máquina pública em favor dos administrados. Ademais, para além de questões relevantes atinentes à qualidade efetiva da informação armazenada, há que se destacar que inexiste forma de coleta de dados que não apresente grau de subjetividade na forma de sistematização do *small data*, seja pela limitação fática quando a dados efetivamente fornecidos, seja pelas análises e inferências que são, a partir deles, realizadas. O efetivo equacionamento entre transparência (espaço público) e sigilo (esfera privada) por meio do que se caracteriza como interesse público preponderante em um dado contexto (elemento de justificação), a partir de uma política pública de privacidade galgada na proteção de dados pessoais, é matéria que, antes de contar com simples resolução apriorística, é permeada por vicissitudes – sobretudo porque tais espaços são rotineiramente sobrepostos no ambiente digital –, cuja parametrização se busca objetivar. Assim, em relação (i) à relação entre privacidade e transparência; (ii) ao uso da automação e a aplicação da inteligência artificial nos processos decisórios; e (iii) ao sopesamento de aspectos históricos, científicos, tecnológicos e estatísticos na tomada de decisão a partir da ótica da proteção de dados pessoais, a fim de contribuir, com base na experiência do TJRS, para o desenho de uma política pública de privacidade.

No âmbito da compatibilidade entre proteção à privacidade e dever de transparência no âmbito público, podem parecer, à primeira vista, contrapostos ou paradoxais os objetivos traçados pelas normas, pois, de um lado, observa-se como preponderante o dever de acesso e compartilhamento de informações impostos pela LAI; de outro, a tônica à proteção de dados por seus titulares. No entanto, um exame acurado dos diplomas e dos fundamentos basilares sob os quais se sustentam permitem se aferir que há caminho passível de harmonização. Em verdade, a preocupação com aspectos

pessoais remonta à edição da LAI que, no seu art. 31, *caput,* já previa a transparência no tratamento de informações pessoais e o respeito à intimidade, vida privada, honra, imagem e liberdades e garantias individuais. Complementa-se a definição de *informações pessoais* (art. 30, § 1º)[111] com o conceito mais abrangente de *dados pessoais* hoje constante da LGPD (art. 5º, I)[112]. Nesse sentido, até mesmo dados cadastrais[113] constantes em bancos nominativos demandam proteção efetiva pela legislação vigente.

A partir dessas premissas, o TJRS estabeleceu, no art. 2º do Ato nº 037/2020, a necessidade de *justificação*, no âmbito interno, da finalidade da realização do ato para propósitos legítimos, explícitos e informados ao titular da informação, inclusive quanto à adequação e necessidade dos meios estabelecidos para o tratamento. É garantido, no âmbito interno da gestão de dados, ressalvadas as *hipóteses justificadas de segredo e sigilo*, segurança pública ou de Estado ou de atividades de atos preparatórios à tomada de dados pessoais (art. 3º), o *livre acesso* aos titulares para o controle da qualidade da transparência dos registros. Esse livre acesso - que pode se manifestar tanto em relação aos dados, quanto em relação ao devido processo informacional (*informational due process*[114]) - é a condição de autonomia fundamental ao sistema, porque permite ao titular da informação o exercício de prerrogativas de ação sobre a informação em qualquer momento do processo de tratamento dos dados pessoais - seja para acessá-lo, seja para controlá-lo, seja para objetá-lo.

Por outro lado, a política pública de privacidade busca garantir a adequação plena dos sistemas e procedimentos internos da LGPD ao mesmo tempo em que se harmoniza com a necessária agilidade na persecução do interesse particular na busca de informações que lhe digam respeito. Daí porque o Ato nº 037/2020-P preconiza, com propriedade, ser viável (i) o uso compartilhado com outras pessoas de direito público, *desde que*

---

[111] Segundo o art. 31, § 1º, da LAI, caracterizam-se como informações pessoais aquelas relativas à intimidade, vida privada, honra e imagem.

[112] Segundo o art. 5º, I, da LGPD, caracterizam-se como dados pessoais qualquer informação relacionada a pessoa natural identificada ou identificável.

[113] Exemplos como CPF, INSS, inscrição de matrícula de servidor junto à sua instituição, dentre outros, muito embora não digam diretamente para com aspectos da vida privada e intimidade, sendo muitos deles até mesmo constantes de dados públicos de acesso, identificam do titular e, por este motivo, são tutelados pela LGPD.

[114] "A partir da tradição norte-americana, também é possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro 'devido processo informacional' (*informational due process privacy right*), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios." Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.389/DF. Brasília, DJ de 07.05.2020. Relatora: Min. Rosa Weber. Excerto de voto: Min. Gilmar Mendes.

justificada a finalidade para o cumprimento de competências legais (art. 7º, § 4º) e (ii) com outras pessoas de direito privado, quando se tratar de dados acessíveis publicamente, *desde que para finalidade compatível com aquela pela qual o acesso foi tornado público* (art. 7º, § 5º, II, do Ato nº 037/2020). Em particular, a norma administrativa se coaduna com a contemporânea contextualização da privacidade na era da informação, dissociando-a da correlação entre privacidade e segredo. Como leciona Solove, "exceto se vivermos como ermitões", não há como existir na atual sociedade sem deixar rastros por onde quer que passemos. (SOLOVE, 2004).

Isto é igualmente relevante, em tempos de automação e de aplicação de uma inteligência artificial forte, a partir do momento em que a atividade administrativa pública sofre transformações, em nome da eficiência, sendo factível a oportunidade de utilização de dados pessoais como base ao aprendizado de sistemas operacionais informatizados. Não é, pois, sem razão, que a política instituída pelo Ato nº 037/2020-P do TJRS busca, paralelamente, contribuir para a *qualificação do processo decisório e de disseminação da cultura de proteção de dados no âmbito da instituição*. A efetiva concretização do *privacy by design* - isto é, do respeito à privacidade desde a concepção de determinado sistema ou processo, de forma uniforme e sistêmica na instituição - é uma preocupação latente. Como ponto de partida do Ato nº 037/2020-P, nos termos da Resolução nº 332/2020 do CNJ, está a necessária *obediência a critérios éticos de transparência, previsibilidade, precaução, auditabilidade, imparcialidade e não discriminação na tomada de decisões automatizadas, em especial quando à qualidade dos dados utilizados em termos de segurança de rede e de fonte, responsabilidade, rastreamento e respeito à privacidade dos usuários*.

Apesar de a inteligência artificial entrar no campo do Direito com função auxiliar – e não substitutiva – aos operadores, a capacidade de tal processo significativo vir a interferir nos processos decisórios administrativos e judiciais é inegável – adquirindo, portanto, funções volitivas -, a exemplo do que já vem sendo noticiado pelo CNJ em vários experimentos realizados no âmbito nacional[115]. A definição ampla do que se entende como IA, nos termos da Resolução do CNJ nº 332/2020, como qualquer conjunto

[115] Os projetos com Inteligência Artificial em andamento junto ao Poder Judiciário são mapeados e podem ser acessados pelo portal https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,currsel Acesso em: 22 jan 2020.

de dados e algoritmos concebidos a partir de modelos matemáticos[116], dialoga de forma direta com a matéria afeta à proteção de dados, pois o comportamento da máquina dependerá das amostras sob as quais o seu aprendizado – de caráter empírico, realizado a partir do reconhecimento de padrões – será conduzido. Nesses termos, "enquanto se convive com a possibilidade real de ultrapassagem da capacidade intelectual humana – leia-se, racionalidade – pelo desenvolvimento de uma racionalidade própria à Inteligência Artificial, urge a necessidade de estabelecimento de garantias à inserção do controle humano nos processos decisórios e automatizados definidos por operações algorítmicas" (CACHAPUZ, 2019, p. 64). Enquanto o livre desenvolvimento da personalidade da pessoa natural insculpido como norte da LGPD em seu art. 1º é atrelado, diretamente, à preservação da autodeterminação informativa, o interesse público no tratamento de dados pessoais implica, especialmente no que toca ao desenvolvimento de algoritmos tendentes ao aperfeiçoamento dos processos decisórios, a criação de salvaguardas para a manutenção efetiva do controle humano, já que as decisões a inferências realizadas têm o condão de impactar drasticamente a universalidade não apenas em um contexto específico, mas com caráter exponencial por meio do caráter de repetição com que determinado padrão é criado, normatizado e replicado em nome de maior segurança jurídica e previsibilidade.

Para além de discussões atinentes aos limites revisionais das decisões automatizadas previstos pela atual redação conferida ao art. 20 da LGPD[117], uma leitura sistemática da internalização da matéria de proteção de dados no âmbito institucional do TJRS zela para que o potencial risco de decisões "caixa-preta"[118] sejam minimizadas por meio do processo de transparência e justificação necessário à sua condução. No Judiciário, o problema maior não seria talvez de origem totalitária – como na distopia de Orwell, pelo interesse de vigilância do indivíduo -, mas sim de caráter cognitivo – como

[116] Segundo o art. 3º, II, da Resolução nº 332/2020 do CNJ, entende-se por modelo de inteligência artificial o "conjunto de dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana".

[117] Fonte de inúmeras preocupações foi a nova redação conferida ao art. 20 da LGPD, ao eliminar a necessidade de que eventual objeção do titular seja realizada por intervenção humana.

[118] O termo *blackbox society* (sociedade caixa-preta), cunhado por Pasquale, apresenta caráter dúplice, pois se refere (i) tanto aos inúmeros dispositivos de vigilância hoje acoplados a aeronaves, trens e automóveis, por exemplo, como (ii) a sistemas cujo funcionamento se apresenta extremamente obscuro. Nesse prisma, sabemos que há uma entrada e saída de informações, mas não temos ideia quanto transitam, como são usadas e quais as suas consequências. (PASQUALE, 2015).

na metáfora de Kafka[119] -, a partir de julgamentos peremptórios e prejudiciais, conforme critérios e perfis estabelecidos a partir de um cruzamento de dados distorcido, por discriminações inerentes ao próprio sistema de tratamento dos dados. Daí a importância de fazer valer, na prática, com caráter permanente, a observância a um princípio de autodeterminação informativa, pela conferência de acesso amplo ao titular dos dados pessoais, inclusive cientificando-lhe previamente quanto aos "procedimentos e as práticas utilizadas para a execução dessas atividades" (art. 7º, caput, do Ato nº 037/2020-P).

De outra parte, conferir conteúdo efetivo ao conceito de interesse público – entendido este como imbricação necessária entre interesses individuais, difusos e coletivos (BASSO, 2020) – revela-se fundamental ao exercício da ponderação, de forma que se possam minimizar situações concretas de conflitos envolvendo privacidade, proteção de dados e publicização de informações. Para além de críticas potenciais em relação ao uso do consequencialismo como método decisório isolado para dirimir sobre a colisão entre direitos fundamentais potencialmente conflitantes – como entre vida privada e acesso à informação –, o princípio da proporcionalidade permite que, por meio de ponderação, seja realizada, de forma antecedente à tomada de qualquer decisão administrativa, uma avaliação dos efeitos concretos relacionados ao tratamento de dados pessoais em contextos específicos, como meio de dimensionar sua adequação, necessidade e proporcionalidade em sentido estrito. É este, aliás, o intuito da elaboração de relatórios de impacto à proteção de dados pessoais (art. 5º, XVII, da LGPD[120]) e da determinação encontrada no art. 13, caput[121] e § 1º, do Ato nº 037/2020-P do TJRS, quando prevê a necessidade de adoção de medidas *suficientes* à comprovação do atendimento às normas de proteção de dados em termos de sua *eficácia, finalidade, metodologia e justificação*.

---

[119] Ao adentrar no tema da privacidade na era informacional, Solove prefere a metáfora de "O Processo", de Franz Kafka a "1984", de George Orwell. Muito embora reconheça a pertinência do *Big Brother* previsto em 1984 para determinados aspectos da sociedade contemporânea, o autor privilegia a noção – e o perigo – de julgamentos prévios e definitivos às pessoas digitais, com impacto direto sobre sua vida, sem terem elas noção mínima da sua existência, pertinência ou adequação. (SOLOVE, 2004).

[120] Relatório de impacto à proteção de dados pessoais é, nos termos do art. 5º, XVII, da LGPD, a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

[121] Na íntegra: Art. 13. Todos que se encontrem na condição de controlador ou operador de dados adotar medidas suficientes, quando necessário, à comprovação do atendimento às normas de proteção de dados pessoais, inclusive quanto à finalidade e eficácia do tratamento.
§ 1.º - Para a demonstração da adequação, devem os agentes de tratamento de dados documentar as operações realizadas, comprovando a metodologia empregada para justificar o alcance da finalidade.

Ciente das dificuldades relacionadas a conflitos potenciais entre titulares de dados e interesses públicos relevantes, como àqueles relacionados a *aspectos históricos, científicos, tecnológicos ou estatísticos à informação de interesse público*, o TJRS estabelece, em seu art. 4º[122], a necessária observância à *suficiente proporcionalidade* à tomada de decisão a eles correlata, *restringindo-se o tratamento de dados pessoais às condições de necessidade e adequação à realização de sua finalidade ao objetivo social e à missão institucional do Poder Judiciário*. A diretriz tem notória relação com a preocupação externada pelo Regulamento (UE) 2016/679, no seu considerando (50), ao demandar que operações para fins de arquivo de interesse público demonstrem comprovação de compatibilidade entre as finalidades (de coleta e de arquivamento), a partir do contexto, da natureza dos dados tratados, das expectativas razoáveis do titular e de suas potenciais consequências.[123]

No momento em que exsurge o papel do agente público também como um mediador de conflitos, sendo "decisiva para a maneira pela qual o público vê o mundo – particularmente, o mundo político – e o seu próprio lugar nele (BASSO, 2020)", a utilização de dados pessoais para finalidades históricas, científicas, tecnológicas ou mesmo estatísticas, apresenta o condão de transposição do princípio da autodeterminação informativa individual para o plano coletivo. Conforme explica Moncau, tais aspectos ressaltam a importância do papel do indivíduo na construção da memória coletiva e, "a

[122] Na íntegra: Art. 4º Observar, no processo de tratamento de dados, suficiente proporcionalidade à tomada de decisão, inclusive quanto aos aspectos históricos, científicos, tecnológicos ou estatísticos à informação de interesse público, restringindo-se o tratamento de dados pessoais às condições de necessidade e adequação à realização de sua finalidade e ao objetivo social e à missão institucional do Poder Judiciário.

[123] As operações de tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, deverão ser consideradas tratamento lícito compatível. (...) A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com **a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento**, após ter cumprido todos os requisitos para a licitude do tratamento inicial, **deverá ter em atenção**, entre outros aspetos, a existência de uma **ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos**, em especial as **expectativas razoáveis do titular dos dados** quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; **a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular**; e a existência de **garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas**. (...) Caso o titular dos dados tenha dado o seu **consentimento** ou o tratamento se baseie em disposições do direito da União ou de um Estado-Membro que constituam uma **medida necessária e proporcionada**, numa sociedade democrática, para salvaguardar, em especial, os importantes objetivos de interesse público geral, o responsável pelo tratamento deverá ser autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades. Em todo o caso, deverá ser garantida a **aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor**. (...) (grifos acrescidos).
Regulamento (UE) 2016/679, considerando (50).

partir dessa construção, que, num processo dialógico, fatos e eventos tornam-se uma memória compartilhada, informando a coletividade e iluminando o caminho das transformações sociais. (MONCAU, 2020)."

Para além de aspectos relacionados à memória, que se relacionam geralmente com fatos históricos, há relevância em se buscar um retrato do presente, ainda mais em uma era onde os dados são abundantes. Nessa linha, ganha relevo a importância da estatística na formulação e aprimoramento de políticas públicas. Quanto ao ponto, emblemáticas são as discussões jurídicas propostas pelas ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, junto ao STF[124], ao tratarem do tema da proteção de dados pessoais, a partir do princípio da autodeterminação informativa, mesmo em momento anterior à vigência da LGPD. Na espécie, a finalidade visivelmente lacônica da Medida Provisória 954/2020[125] - que obrigava o compartilhamento de dados pessoais por empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE) durante o estado de calamidade pública da pandemia da COVID-19 -, foi o principal elemento a demonstrar a inconstitucionalidade flagrante do ato. Nos dizeres da relatora do caso, o interesse público estatístico da coleta restava demasiadamente fragilizado, na medida em que "ao não definir apropriadamente como e para que serão usados os dados coletados, a Medida Provisória não oferece condições para avaliação da sua adequação e necessidade[126]." Posto de outro modo: *o que se inviabiliza*, quando da finalidade demasiadamente ampla a um tratamento maciço de dados pessoais, *é o próprio exame da proporcionalidade*. Há, de um lado, a restrição à privacidade sem se ter, em contrapartida, a ponderação por peso do interesse público que se está a salvaguardar. Sem se ter a equação da ponderação necessária, inviável se mostra a restrição a qualquer direito fundamental *a priori*.

---

[124] Ações reunidas por pertinência temática. Discussão traçada no Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF. Brasília, DJ de 07.05.2020. Relatora: Min. Rosa Weber.

[125] Para melhor explicitação da problemática enfrentada, relaciona-se a íntegra de dispositivo que demonstrava a finalidade e extensão dos dados pessoais a serem compartilhados: Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.

§ 1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

§ 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o caput.

§ 3º Os dados deverão ser disponibilizados no prazo de:

I - sete dias, contado da data de publicação do ato de que trata o § 2º; e

II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes.

[126] Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF. Brasília, DJ de 07.05.2020. Relatora: Min. Rosa Weber.

No âmago dessa aparente contraposição entre interesses pessoais e coletivos, está a base concreta para a aplicação prática do princípio da transparência na ponderação de aspectos históricos, científicos, estatísticos e tecnológicos quando da tomada de decisão. Tais fatos contribuem não apenas para o fortalecimento dos instrumentos democráticos em sociedade, mas também para que liberdades sejam compatibilizadas no agir social. Não, portanto, porque se reconheça uma precedência do interesse público desde sempre. Mas sim, porque efetuadas as ponderações necessárias e suficientes, pelas condições fáticas e jurídicas oferecidas pelo caso, quando da tomada de decisão administrativa. É com isso, ao final, que se preocupa o ato administrativo editado pelo TJRS.

3. Conclusões

Em reflexão icônica, Marilyn Monroe prenunciou-se, em certa ocasião, quanto às agruras da exposição restritiva de privacidade a que a pessoa pública está adstrita: "Eu sabia que eu pertencia ao público e ao mundo, não porque eu fosse talentosa ou mesmo bonita, mas porque eu nunca pertenci a nada ou mais ninguém.[127]" A questão ao fundo é, na essência, como referiria Hannah Arendt, o problema do "impulso à auto-exposição" (ARENDT, 1993, p. 28), não apenas porque a pessoa participa de uma vida comum com os demais, compartilhando experiência tecnológica e informações próprias a seu tempo, mas, fundamentalmente, porque também o indivíduo deseja *aparecer* e, em determinada medida, fazer-se visto, "por feitos e palavras" (ARENDT, 1993, p. 28), pelos demais[128].

Entre Monroe e o caso do IBGE que chegou à discussão junto ao STF, estão os contextos e os interesses públicos que os parametrizam, por entre liberdades positivas e negativas. É, portanto, por meio de uma tomada de decisão justificada, a partir da ponderação realizada para o caso, que o Poder Público se vê autorizado a desempenhar uma função prospectiva, identificada pelo compromisso de coerência e consistência com o sistema, corrigindo-o para futuro e respeitando aquilo que adquire estabilidade pela consolidação jurisprudencial, judicial ou administrativa, em observância à sua atribuição como fonte normativa do Direito (art. 7º, § 2º, III, do Ato nº 037/2020-P do TJRS).

Na essência, é o que potencializa, de forma específica, o exercício pleno da autodeterminação informativa - que, ao fundo, espelha a própria ideia de autonomia do

[127] Tradução livre. Original: "I knew I belonged to the Public and to the world, not because I was talented or even beautiful but because I had never belonged to anything or anyone else." (MONROE, 2000. p. 123-24).

[128] No tema, ver estudo sobre liberdade e acesso à informação, pela análise da "autodeterminação informacional", em Tércio Sampaio Ferraz Júnior (2001, p. 242).

indivíduo, aplicada ao tema da proteção de dados pessoais. Não muito diferente, portanto, do que Habermas reconheceu como pressuposto à dupla dinâmica de enfoque em relação à dimensão de autonomia do indivíduo - como individualidade e como intersubjetividade -, aproximando a discussão filosófica do campo de análise da liberdade em termos jurídicos. Quando se fala em *autonomia*, seguindo Habermas, se está, em verdade, discutindo questão mais ampla que a pressuposta num direito geral de liberdade, diferenciando-se os conceitos pelo âmbito de sua abrangência. Enquanto a liberdade é sempre subjetiva, porque fundada nas peculiaridades do indivíduo – suas "máximas de prudência, pelas preferências ou motivos racionais" (HABERMAS, 2004) -, a autonomia é um conceito que pressupõe uma estrutura de intersubjetividade, determinada por máximas aprovadas pelo teste da universalização (HABERMAS, 2004, p. 13).

Isso significa compreender que, para efeito de análise do problema posto dentro das bases de estabelecimento de uma política pública de efetiva proteção à privacidade e a dados nominativos, ainda que se possa reconhecer a liberdade do indivíduo em abstrato, é necessário que lhe seja possível visualizar também autonomia em potencial. O que exige o reconhecimento expresso, por políticas públicas, de uma autodeterminação informativa a todo titular de dados informativos. Só assim resta autorizada a percepção de que a pessoa é participante de uma comunidade moral ou, como prefere Habermas, de "uma comunidade formada de indivíduos livres e iguais, que se sentem obrigados a tratar uns aos outros como fins em si mesmos" (HABERMAS, 2004, p. 13).

4. Referências Bibliográficas

ALEXY, Robert. **Teoría de los derechos fundamentales**. Madrid, CEPC, 2001.

ARENDT, Hannah. **A vida do espírito: o pensar, o querer, o julgar**, 2ª edição. Rio de Janeiro, Relume Dumará, 1993.

___. Public rights and private interests: In response to Charles Frankel. In: MOONEY, M.; STUBER, F. **Small comforts for hard times. Humanists on public policy**. New York, Columbia University Press, 1977.

___. **Responsabilidade e julgamento.** São Paulo, Companhia das Letras, 2004.

BASSO, Bruno Bartelle. Direito à privacidade e o tratamento de dados pessoais pelo poder público: o interesse público como elemento dialógico da relação. In: POZZO, Augusto e

CACHAPUZ, Maria Cláudia. **A obrigação pelo discurso jurídico. A argumentação em temas de Direito Privado**. Porto Alegre, Sergio Antonio Fabris Editor, 2018.

___. Informática e proteção de dados. Os freios necessários à automação. **Revista da Ajuris**, ano XXIV, vol. 70, julho 1997.

___. **Intimidade e vida privada no novo Código Civil brasileiro. Uma leitura orientada no discurso jurídico.** Porto Alegre, Sergio Antonio Fabris Editor, 2006.

___. O conceito de pessoa e a autonomia de Data (ou sobre a medida da humanidade em tempos de inteligência artificial. **Revista de Direito Civil Contemporâneo** nº 20, 2019, p. 63-86

CASTELLS, Manuel. **A sociedade em rede - A era da informação**: Economia, sociedade e cultura (vol. I), 2ª edição. São Paulo, Paz e Terra, 1999.

CATE, Fred H. **Privacy in the information age**. Washington, DC, Brookings Institution Press, 1997.

EIRAS, Agostinho. **Segredo de justiça e controlo de dados pessoais informatizados**. Coimbra, Coimbra Editora, 1992.

FERRAZ JR., Tércio Sampaio. A liberdade como autonomia de acesso à informação. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (org.). **Direito e Internet: relações jurídicas na sociedade informatizada**. São Paulo, Revista dos Tribunais, 2001.

FRAYSSINET, Jean; KAYSER, Pierre. A lei de 06 de agosto de 1978, relativa à Informática, fichários e liberdades e o decreto de 17 de julho de 1978. **RPGE**, 13 (35), Porto Alegre, 1983.

FROMM, Erich. **O medo à liberdade**, 9 ed. Rio de Janeiro, Zahar, 1974.

GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (org.). **Direito e Internet**: **relações jurídicas na sociedade informatizada**. São Paulo, Revista dos Tribunais, 2001.

HABERMAS, Jürgen. **A ética da discussão e a questão da verdade**. São Paulo, Martins Fontes, 2004.

KERBER, L. K. The Meanings of Citizenship. In: **The Journal of American History**, 84(3), 833, 1997.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da informática**. Coimbra, Livraria Almedina, 2000.

MARTINS, Ricardo (coord). **LGPD e Administração Pública** – Uma análise ampla dos impactos. E-book. São Paulo: RT, 2020.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: a revolution that will transform how we live, work, and think.** First Mariner Books: New York, 2014, p. 15 e p. 73 – 98.

MONCAU, Luiz Fernando. **Entre a Liberdade de Expressão, a Privacidade e a Proteção de Dados Pessoais**. E-book. São Paulo: RT, 2020.
MONROE, Marilyn. **My Story**. New York, Cooper Square Press, 2000.

OCDE. **A Caminho da Era Digital no Brasil.** OECD Publishing: Paris, 2020. https://doi.org/10.1787/45a84b29-pt.

ORTIZ, Ana Isabel Herrán. **El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales**. Madrid, Dykinson, 2002.

PASQUALE, Frank. **The Black Box Society.** London: Harvard University Press, 2015.

SCHWABE, Jürgen. **Cincuenta años de jurisprudencia del Tribunal Constitucional Federal alemán.** Montevideo, Konrad-Adenauer-Stiftung, 2003.

SOLOVE, Daniel. **The Digital Person**: Technology and Privacy in the Information Age. New York University Press: New York, 2004.
___. **La violación de la intimidad en la protección de datos personales**. Madrid, Dykinson, 1998.

VIRILIO, Paul. **A bomba informática**. São Paulo, Estação Liberdade, 1999.

A Lei Geral de Proteção de Dados Pessoais e os seus reflexos no Poder Judiciário brasileiro

Luciano Alves dos Santos[129]

RESUMO

O advento da Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709, de 14 de agosto de 2018 e suas posteriores alterações, fez aumentar a complexidade da proteção aos dados dos jurisdicionados, bem como dos servidores e juízes vinculados aos tribunais brasileiros. Essa nova legislação, baseada em grande parte no Regulamento Geral sobre a Proteção de Dados existente na Europa, apresenta uma série de desafios ao Poder Judiciário brasileiro, pois as adequações, reorganizações e mudanças na cultura da proteção de dados, assim como a implantação ou ampliação do *compliance* digital, com a finalidade de proteger de vazamentos e má utilização, os dados presentes em seus sistemas e convênios, confiados a esse Poder Estatal de boa-fé e com a confiança de que serão preservados e bem geridos, estando a personalidade e a dignidade de quem integra uma lide protegidas de investidas de hackers ou pessoas e entidade que possam, de alguma forma, lucrar com a comercialização desses dados, ou até mesmo infligir algum dano, seja moral ou material ao usuário do sistema.

Face a esse novo contexto, a Administração Pública e, no caso específico, o Poder Judiciário brasileiro estão tomando medidas para se adequarem a esta nova realidade, que visa dar concretude a normas contidas na Constituição Federal de 1988, buscando, inclusive, harmonização hermenêutica com a legislação pré-existente, com destaque para a Lei de Acesso à Informação, Lei n.º 12.527/2011, a qual, aparentemente, se choca com algumas determinações da Lei Geral de Proteção de Dados Pessoais.

PALAVRAS-CHAVE

Lei Geral de Proteção de Dados Pessoais; Poder Judiciário Brasileiro; Adequação: Reflexos.

[129] Mestre em Direito pela URI-Campus Santo Ângelo-RS. Pós-graduado em Inovações do Direito pela UNISUL-SC. Bacharel em Direito pela Universidade Federal de Pelotas-RS (UFPEL). Professor de Direito Internacional Público e Privado na URI-Campus Erechim. Servidor da Justiça Federal na Subseção Judiciária de Erechim, onde desenvolve a Supervisão do CEJUSCON (Centro Judiciário de Solução de Conflitos e Cidadania). Membro do Grupo de Pesquisa Direito Transnacional nas Relações Jurídicas Atuais com Ênfase no Direito Digital/Informacional. E-mail: *lucianoa@uricer.edu.br*. Currículo lattes: http://lattes.cnpq.br/8996637354776615.

The General Law on the Protection of Personal Data and its effects on the Brazilian Judiciary

ABSTRACT

The advent of the General Law on the Protection of Personal Data, Law No. 13,709, of August 14, 2018 and its subsequent amendments, increased the complexity of data protection for jurisdictional authorities, as well as for civil servants and judges linked to Brazilian courts. This new legislation, based largely on the General Regulation on Data Protection in Europe, presents a series of challenges to the Brazilian Judiciary, as the adjustments, reorganizations and changes in the culture of data protection, as well as the implementation or expansion of digital compliance, with the purpose of protecting from leaks and misuse, the data present in its systems and agreements, entrusted to this State Power in good faith and with the confidence that they will be preserved and well managed, with personality and dignity of those who are part of a process protected from attacks by hackers or individuals and entities that may, in some way, profit from the commercialization of this data, or even inflict any damage, whether moral or material, to the system user.

In view of this new context, the Public Administration and, in the specific case, the Brazilian Judiciary are taking measures to adapt to this new reality, which aims to give concreteness to the rules contained in the Federal Constitution of 1988, seeking, also, hermeneutic harmonization with the pre-existing legislation, with emphasis on the Access to Information Law, Law No. 12,527 / 2011, which, apparently, clashes with some determinations of the General Law on Protection of Personal Data.

KEYWORDS

General Law of Protection of Personal Data; Brazilian Judiciary; Adequacy; Reflexes.

Introdução

O presente artigo surgiu a partir de convite para realizar uma conferência no *Privacy and Data Protection Centre*, da Universidade Europeia em Lisboa, no dia 03 de dezembro de 2020, na qual desenvolvi o tema: A LGPD e os seus Reflexos no Poder Judiciário brasileiro, convite este vindo da parte da Caríssima Professora Dra. Cristina Maria de Gouveia Caldeira, no webinar, com o título "O RGPD, a LGPD e os seus reflexos no Poder Judiciário Brasileiro", ao lado da ilustre Professora Dra. Elizabeth Accioly.

O objetivo da fala foi demonstrar quais as dificuldades e desafios enfrentados pelo Judiciário brasileiro na adaptação à recente Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709, de 14 de agosto de 2018, alterada pela Lei n.º 13.853, de 08 de julho de 2019), a qual passou a viger em 18 de setembro de 2020.

Baumann (2001, p. 213) enfatiza que "[...] A liberdade da política do Estado é incansavelmente erodida pelos novos poderes globais providos das terríveis armas da extraterritorialidade, velocidade de movimento e capacidade de evasão e fuga", o que hodiernamente é algo real, pois, por várias vezes e, em diversos momentos, tem havido ataques endógenos e exógenos a dados pessoais de cidadãos mantidos em posse, tanto de organizações privadas, quanto públicas.

Com essa preocupação, o legislador brasileiro criou a Lei Geral de Proteção de Dados (LGPD), que trouxe e ainda traz diversos desafios aos entes públicos e privados.

No presente artigo será apresentada a LGPD, bem como os desafios que esta apresenta ao Poder Judiciário para a sua adequada e efetiva implementação, respeitando os ditames constitucionais e harmonizando-se com a legislação pré-existente.

1. A Lei Geral de Proteção de Dados no Brasil

No ano de 2010, o Ministério da Justiça começou a discussão acerca do que seria a futura LGPD ao efetuar a primeira consulta pública de um Anteprojeto de Lei de Proteção de Dados Pessoais no site culturadigital.br, o que com o passar do tempo evoluiu para o Projeto de Lei 4060/2012 CAM, proposto pelo Deputado Milton Monti. Já em 2013, houve os dados revelados por Edward Snowden, o que acelerou a aprovação do Marco Civil da Internet e o transformou em um microssistema de proteção de dados pessoais aplicáveis ao setor de Internet (BIONI, 2018).

O mesmo autor destaca que no ano de 2015 foi lançado um segundo processo de consulta pública, de um novo anteprojeto de lei de proteção de dados pessoais, ao que, nesse momento, já atingia um nível mais qualificado de discussão, inclusive por conta do

maior e melhor engajamento da participação pública em comparação com o processo de 2010. Dessa forma, nasce já bastante maduro, o que viria a ser a base do PLC 53/2018, o qual foi encaminhado à Câmara dos Deputados e se transformou no PL 5276/2016.

Bioni (2018) informa que "desde logo, tal iniciativa legislativa contou com o apoio de mais de 40 (quarenta) entidades nacionais e internacionais (...)", sendo que tais entidades afirmavam que se tratava de uma redação equilibrada a salvaguardar a inovação e a proteção da privacidade dos cidadãos.

Para que o texto não fique cansativo, sugere-se verificar todo o trâmite do processo no artigo referido, o que pode ser feito acessando o site colocado nas referências do texto ou acessando o QR CODE, ao lado.

Ao fim do processo, brevemente descrito acima, nasceu a Lei n.º 13.709, de 14 de agosto de 2018, que foi alterada pela Lei n.º 13853, de 2019, passando então a se chamar Lei Geral de Proteção de Dados Pessoais.

Tal lei vem se incorporar ao arcabouço protetivo do cidadão brasileiro em relação a possíveis abusos envolvendo seus dados pessoais, sua identidade, sua privacidade e, por fim e mormente, sua dignidade.

É de se ressaltar que a LGPD traz em seu bojo a definição de alguns conceitos importantes, como o de titular dos dados pessoais, de controlador, de tratamento de dados, entre outros, os quais serão tratados posteriormente.

2. Principais conceitos trazidos pela LGPD e do que tratam seus artigos

O Serviço Federal de Processamento de Dados (SERPRO) resume em um infográfico, denominado: "A LGPD em um giro", os principais aspectos da lei, veja-se:

Fonte: SERPRO, 2020.

Para melhor compreensão do que trata cada parte da lei, segue a indicação do conteúdo dos artigos ou de alguns grupos deles:

> Objetivo (Art. 1º); Fundamentos (Art. 2º); Âmbito de aplicação (Art. 3º); Exceções (Art. 4º); Definições (Art. 5º); Princípios (Art. 6º); Tratamento de Dados Pessoais (Art. 7º a 10º); Tratamento de Dados Pessoais Sensíveis (Art. 11 a 13); Tratamento de Dados Pessoais de Crianças e Adolescentes (Art. 14); Término do Tratamento de Dados (Art. 15 e 16); Direitos do Titular (Art. 17 a 22); Tratamento de Dados Pessoais pelo Poder Público (Art. 23 a 32); Transferência Internacional de Dados (Art. 33 a 36); Agentes de tratamento de Dados Pessoais (Art. 37 a 45); Segurança e boas práticas (Art. 46 a 51); Fiscalização (Art. 52 a 54); Autoridade Nacional de Proteção de Dados (ANPD) e Conselho Nacional de Dados Pessoais e da Privacidade (Art. 55-A a 58-B) e Disposições Finais e Transitórias (Art. 60 a 65).

O Art. 5º da LGPD apresenta vários conceitos importantes, conforme abaixo, enumeram-se:

> I – **dado pessoal:** informação relacionada à pessoa natural identificada ou identificável;
>
> **II – dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> **III – dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> **IV – banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> **V – titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> **VI – controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> **VII – operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> **VIII – encarregado:** pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;
>
> **VIII – encarregado:** pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (Redação dada pela Medida Provisória nº 869, de 2018)
>
> **VIII – encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)
>
> **IX – agentes de tratamento:** o controlador e o operador;
>
> **X – tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII – bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI – uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou

aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Medida Provisória nº 869, de 2018)

XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

XIX – autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2018)

XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

Tais conceitos trazidos pela lei são importantes para a determinação das funções, responsabilidades e direitos de cada uma das *personas* envolvidas neste contexto.

3. Abrangência da LGPD

Muito embora não seja possível contestar a necessidade de um regime jurídico de proteção de dados, no Brasil, similar ao RGPD, é muito claro que a implantação e efetividade da LGPD está sendo um grande desafio para a gestão pública nacional, inclusive para os tribunais.

Não seria exagero afirmar que os desafios oferecidos pela LGPD aos entes públicos são sensivelmente maiores se comparados com aqueles introduzidos pela Lei de Acesso à Informação (LAI). Isto porque, no caso da LAI, como regra, os dados já se encontravam à disposição da Administração Pública, cabendo a esta, dar-lhes publicidade, nos moldes preconizados pela novel legislação (transparência passiva e ativa), ao passo que no caso da LGPD muitas operações de tratamento de dados sequer são compreendidas como tal no âmbito da Administração Pública. (PUGLIESI, 2020).

O grande desafio será determinar, especificamente, o papel de cada agente, o que certamente compreenderá a necessidade de alteração de cultura organizacional, inclusive

trazendo a toma a necessidade de conciliação da LGPD com o princípio da publicidade, consagrado no art. 37 da Constituição Federal de 1988 e, ainda, com os ditames da Lei de Acesso à Informação.

Inclusive, haverá maior necessidade de estabelecimento de regras claras de *Compliance* Digital, conforme cita Lopes (2020):

> Compliance, em tradução livre, é o mais próximo de "conformidade", assim, relaciona-se diretamente com a devida aplicação das normas, leis, regimentos e diretrizes, sejam internas (como um Regimento Interno ou Código de Conduta e Ética), sejam externas (com a devida aplicação das leis municipais, estaduais e federais), bem como a prevenção no caso de não aplicação destas, analisando seus riscos e impactos no ambiente. Nesse sentido, compliance digital tem como função a análise dos riscos e a criação de medidas de prevenção para conformidade com regras, condutas e ética aplicáveis à tecnologia de informação, o que podemos incluir desde proteção de dados, direito autorais, crimes cibernéticos e direito de privacidade em âmbito digital.

O autor ainda trata dos riscos que se podem mitigar a partir da adoção do *Compliance* Digital, quais sejam:

> **I. Uso indevido de ferramentas e programas digitais**: como utilização incorreta das mídias digitais, postagens de caráter ofensivo e/ou enganoso, ou mesmo a utilização de programas pirateados no computador;
>
> **II. Uso de conteúdo protegido**: como imagens, textos, artigos, entre outras fontes e mídias que estão disponíveis na internet e aparentam não possuir direitos autorais e, por sua, vez, estampam sites, blogs, divulgação de produtos e mídias digitais de empresas desavisadas;
>
> **III. Malwares**: todo e qualquer arquivo ou aplicativo que possui comportamento malicioso e nocivo para o usuário (como vírus, ransomwares e worms);
>
> **IV. Phishing**: sites e aplicativos falsos que têm por objetivo enganar os usuários para coletarem informações importantes, como senhas ou arquivos confidenciais;
>
> **V. Crimes cibernéticos**: que podem ser cometidos por funcionários, dirigentes ou mesmo prestadores de serviços, ou contra eles e a empresa;
>
> **VI. Perfis falsos em redes sociais**: que podem, ilegal e injustamente, difamar pessoas ou empresas;
>
> **VII. Domínios similares**: cópias do site ou domínios com grande semelhança ao original que possam ser utilizados com o intuito de enganar usuários;
>
> **VIII. Vendas não autorizadas**, entre outras situações recorrentes no dia a dia de uma empresa que possui o mínimo de acesso a um sistema digital.

Esses, porém, são somente alguns exemplos dos riscos existentes, pois na prática são incontáveis; porém, com o avanço da tecnologia, surgem sempre novas ameaças.

Assim, será necessária uma verdadeira mudança cultural para que se possam minorar os riscos advindos das atividades diárias inerentes à administração pública, mormente, em relação ao foco principal do presente artigo: a atividade judiciária.

4. Art. 37 da Constituição Federal de 1988, Lei de Acesso à Informação e Lei Geral de Proteção de Dados Pessoais: será possível conciliá-los?

A Lei de Acesso à Informação, Lei n.º 12.527/2011 (BRASIL), cita em seu artigo 1º, o inciso II, do §3º do art. 37 da Constituição Federal o qual determina o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, 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) e XXXIII (todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado). Inclusive, a Lei de Acesso à Informação vem para regulamentar o inciso XXXIII, do art. 5º da Constituição Federal de 1988 (BRASIL).

Assim, no primeiro momento tem-se o que, aparentemente, seria um conflito entre a publicidade, determinada pela Constituição Federal e regulamentada pela Lei de Acesso à Informação, e a proteção de dados, determinada pela LGPD.

É de ser ressaltada a existência de julgados importantes, anteriores à LGPD, como o ARE 652.777, no qual o Supremo Tribunal Federal determina a publicidade, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes de seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias (BRASIL, 2015).

Nesse contexto, surge a seguinte questão: como conciliar a proteção de dados pessoais havendo determinação de sua publicização?

Dessa forma, citam-se as palavras de Pugliesi (2020), quanto à temática:

> Como se não bastasse, a introdução da LGPD no setor público deve conciliar os fundamentos que lhes são próprios, tais como o respeito à privacidade, a inviolabilidade da intimidade, da honra e imagem (artigo 2º, I e IV), com os princípios da publicidade consagrados tanto no artigo 37, *caput*, da Constituição Federal quanto na LAI.
>
> Trata-se, em outras de palavras, de buscar a adequação entre a transparência que deve reger as atividades da Administração Pública e o regime jurídico de

> proteção de dados inaugurado pela LGPD, o que, certamente, traduz um grande desafio ao gestor público.
>
> Pensamos que alguns instrumentos previstos na LGPD, tais como a anonimização ou a pseudonimização, podem ser úteis ao gestor público, vez que possibilitará a divulgação de documentos sem, contudo, permitir a identificação de dados pessoais dos indivíduos envolvidos, nos casos em que a publicidade integral não derive de expressa disposição legal.

Defende-se que, em verdade, haja uma ponderação em relação ao que deve ser divulgado e ao que deve permanecer em sigilo, ou seja, há que se fazer uma análise de forma a interligar, conectar as legislações existentes, compatibilizando-as, não as colocando em choque, pois há diversas formas de se publicizar um dado, sem atentar contra a dignidade de alguém.

5. A LGPD e sua implementação no Poder Judiciário

O Poder Judiciário, assim como toda a Administração Pública brasileira, está enfrentando a complexidade e os desafios trazidos pela LGPD, pois ela demanda a (re)adequação de suas normas internas e de sua práxis, pois a legislação nacional infraconstitucional permite várias situações, as quais se abordarão a título exemplificativo, mais adiante.

É importante referir que o Judiciário brasileiro está adequando-se à LGPD, via normatização expedida pelo Conselho Nacional de Justiça (CNJ), o qual, durante a sua 323ª sessão ordinária, em 15 de dezembro de 2020, aprovou uma resolução que padroniza os critérios dos tribunais brasileiros (com exceção do Supremo Tribunal Federal) para adequação à LGPD, indicando que cada tribunal deverá criar um Comitê Gestor de Proteção de Dados Pessoas (CGPD), órgão que será responsável pela implementação da lei, inclusive analisando o compartilhamento de dados em contratos e convênios. (CONJUR, 2020).

Cardoso (2020), em artigo denominado "A regulamentação da proteção de dados pessoais pelo Conselho Nacional de Justiça", informa que tal ato normativo define treze medidas, em seu art. 1º, para serem adotadas em todos os tribunais brasileiros, exceto o Supremo Tribunal Federal, conforme anteriormente referido, as quais, passa-se a listar:

> (a) a criação do Comitê Gestor de Proteção de Dados Pessoais (CGPD) em cada tribunal, com caráter multidisciplinar, que será o órgão responsável pelo processo de implantação da LGPD (na primeira e segunda instâncias, além dos tribunais superiores);
>
> (b) a designação do encarregado pelo tratamento de dados pessoais;

(c) a formação de um Grupo de Trabalho Técnico, com caráter multidisciplinar (composto por servidores das áreas de tecnologia, segurança da informação e jurídica, entre outras), para auxiliar o encarregado no desempenho de suas funções;

(d) a elaboração, por meio de canal do encarregado (ou em parceria com a ouvidoria do tribunal): (d.1) de um formulário eletrônico ou de um sistema para atendimento das requisições e/ou reclamações apresentadas pelos titulares dos dados pessoais; (d.2) e de um fluxo para atendimento aos direitos dos titulares, da apresentação das requisições e/ou reclamações até a prestação da resposta;

(e) a criação de uma seção dentro do site do tribunal contendo informações sobre a aplicação da LGPD na Corte, que deve conter em seu conteúdo mínimo: (e.1) as bases legais utilizadas para o tratamento de dados pessoais; (e.2) os deveres dos controladores e os direitos dos titulares (de acordo com o art. 1º, II, 'a', da Recomendação nº 73/2020 do CNJ; (e.3) e as informações sobre o encarregado (nome, endereço e e-mail para contato);

(f) a disponibilização de informações adequadas sobre o tratamento de dados pessoais, por meio de: (f;1) avisos de *cookies* no portal institucional do tribunal; (f;2) política de privacidade para navegação na página da instituição; (f;3) e política geral de privacidade e proteção de dados pessoais a ser aplicada internamente em cada tribunal e supervisionada pelo Comitê Gestor de Proteção de Dados Pessoais;

(g) a criação dos assuntos suplementares "proteção de dados pessoais" e "privacidade" nas tabelas processuais, para facilitar a distribuição e o controle das demandas relacionadas à proteção de dados, ao respeito à privacidade e à LGPD;

(h) a determinação de análise pelos serviços extrajudiciais sobre a adequação de suas atribuições à LGPD;

(i) a organização de um programa de conscientização sobre a LGPD, destinado a magistrados, servidores, terceirizados, estagiários e residentes judiciais, das áreas administrativas e judiciárias de primeira e segunda instâncias;

(j) a revisão de todos os modelos de minutas de contratos e convênios em vigor que autorizem o compartilhamento de dados com terceiros, e a elaboração de orientações para a adequação das contratações futuras à LGPD, a partir dos seguintes critérios: (j.1) cada operação de tratamento de dados pessoais deve conter uma finalidade específica, vinculada ao interesse público e apoiada em uma

regra de atribuição administrativa aplicável ao caso; (j.2) o tratamento de dados pessoais previsto no ato deve ser compatível com a finalidade especificada e necessário para a sua realização; (j.3) a inclusão de cláusulas de eliminação de dados pessoais nos contratos, convênios e instrumentos congêneres, observados os princípios da finalidade e da necessidade; (j.4) e a elaboração do relatório de impacto de proteção de dados pessoais previamente ao contrato ou convênio, observado o princípio da transparência;

(k) a implantação de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, por meio da: (k.1) elaboração de política de segurança da informação, que contenha um plano de resposta a incidentes (art. 48 da LGPD), e a previsão de adoção de mecanismos de segurança desde a concepção de novos produtos ou serviços (art. 46, § 1º, da LGPD); (k.2) avaliação dos sistemas e dos bancos de dados em que houver tratamento de dados pessoais, com a submissão dos resultados à apreciação do CGPD para as devidas deliberações; (k.3) avaliação da segurança de integrações de sistemas; (k.4) análise da segurança das hipóteses de compartilhamento de dados pessoais com terceiros;

(l) a elaboração e a manutenção dos registros de tratamentos de dados pessoais, com informações sobre a finalidade do tratamento, a base legal; a descrição dos titulares, as categorias de dados, as categorias de destinatários, a eventual transferência internacional; o prazo de conservação e as medidas de segurança adotadas (art. 37 da LGPD);

(m) e a prestação das informações ao Comitê Gestor de Proteção de Dados Pessoais sobre a existência de projetos de automação e inteligência artificial, com a elaboração do relatório de impacto à proteção de dados pessoais relativo aos critérios e direitos previstos na LGPD (art. 6º, VI e IX, e art. 20). Cardoso 2020) ainda refere que o art. 2º da Resolução estabelece três ações mínimas que os tribunais devem observar para a implantação da LGPD, quais sejam:

> (1) a realização do mapeamento de todas as atividades de tratamento de dados pessoais, por meio do modelo de questionário a ser elaborado pelo CNJ;
> (2) a realização da avaliação das vulnerabilidades (*gap assessment*) para o diagnóstico das lacunas existentes na proteção de dados pessoais;

> (3) e a elaboração de um plano de ação (*roadmap*), com a previsão de execução de todas as atividades previstas na Resolução.

Por fim, o citado autor indica que a Resolução, acima tratada, carrega conteúdo de Recomendação, porque não regulamenta a aplicação da LGPD no Judiciário, mas contém regras gerais que orientam os tribunais a adequarem as suas atividades à Lei Geral de Proteção de Dados Pessoais (de modo similar à Recomendação nº 73/2020 do CNJ), como a criação do Comitê Gestor e do Grupo de Trabalho, a inclusão do portal de proteção de dados na internet, a revisão de atos e contratos, a documentação das atividades de tratamento e a adoção de ações mínimas para o cumprimento adequado das normas legais.

Assim, cada tribunal deve criar sua própria regulamentação, para situações como a gravação de audiências, permitida pelo Código de Processo Civil no Art. 367, §5º e no Código de Processo Penal, no Art. 405, §1º, pois caso salve estes arquivos em uma nuvem, por exemplo, não estaria criando um novo operador? E como ficaria a questão do segredo de justiça em relação ao acesso a estes arquivos por pessoa ou organização alheia ao Judiciário, partes e procuradores que atuem no processo?

São questões como essas, em números expressivos, que estão, neste momento, tratando os tribunais brasileiros; adequando seus ordenamentos internos, sua política de proteção de dados, além de estarem trabalhando em formação e alteração de cultura de segurança e uso de dados por parte de seus Juízes e Servidores.

Essa afirmação é feita baseada em levantamento efetuado por Valente (2020) que dentre os tribunais superiores, regionais federais e estaduais, apenas dois consideram que já estão adequados à LGPD: o Tribunal de Justiça de São Paulo e o de Minas Gerais, sendo tal levantamento de novembro de 2020.

Com base no mesmo levantamento, as maiores dificuldades relatadas, em geral, tratam de mudança de cultura para reestruturação dos processos internos e a falta de diretrizes nacionais específicas para o Judiciário (o que foi possivelmente sanado, com a Resolução do CNJ de 15 de dezembro de 2020).

Além disso, destacam: o volume de dados, a diversidade de sistemas, de resoluções e de fluxos de dados pessoais e, ainda, a conformidade com a lei para documentos não estruturados, sendo que a maioria dos tribunais prevê a adequação para até a meados de 2021.

O levantamento indica que, com exceção dos tribunais do Amazonas, Goiás e Minas Gerais, todos os demais afirmaram que integram alguma rede ou grupo para compartilhamento de informações. A troca acontece, em suma, com outros tribunais, na Plataforma de Governança Digital Colaborativa do Poder Judiciário e na Base Nacional de Dados do Poder Judiciário (DataJud).

6. Considerações finais

O presente estudo buscou apresentar um panorama geral sobre o estado atual e os desafios presentes e vindouros que se antepõem à efetivação da real proteção buscada pelo legislador, quando da criação da LGPD. Esse trabalho tem a finalidade de instigar futuras investigações sobre o tema, verificando-se o estado posterior à implementação dessa norma protetiva na atividade cotidiana dos tribunais brasileiros.

Nesse contexto, pode-se observar que o Poder Judiciário brasileiro está em vias de adequação às determinações trazidas pela LGPD, tratando-se de verdadeira (r)evolução no tocante à proteção de dados dos seus usuários (jurisdicionados, servidores e juízes), bem como, ao fim e ao cabo, protegendo a dignidade da pessoa humana (Art. 1º, III, da Constituição Federal) e realizando os ditames do Art. 5º, X, da Constituição Federal, que determina que – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação.

7. Referências bibliográficas

BAUMANN, Zygmunt - **Modernidade Líquida**. Trad. DENTZIEN, Plínio. Jorge Zahar Editor. Rio de Janeiro. 2001.

BRASIL **- Constituição Federal da República Federativa do Brasil de 1988**. [04 Jan. 2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

_____ - Supremo Tribunal Federal. **ARE 652.777**. Julgado em 23/04/2015. [06 Jan. 2021]. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8831570.

_____ **- Lei n.º 12.527, de 18 de novembro de 2011** – **Lei de Acesso à Informação.** [06 Jan. 2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

_____ **- Lei n.º 13.709, de 14 de agosto de 2018** – **Lei Geral de Proteção de Dados Pessoais (LGPD)**. [06 Jan. 2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BIONI, Bruno R - **De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados.** [09 Jan. 2021]. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-

da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018.

CARDOSO, Oscar Valente - **A regulamentação da proteção de dados pessoais pelo Conselho Nacional de Justiça.** Revista Jus Navigandi, Teresina, ano 25, n. 6377, 16 dez. 2020. [09 Jan. 2021]. Disponível em: https://jus.com.br/artigos/87452. ISSN 1518-4862.

CONJU - **CNJ aprova resolução que padroniza adequação dos tribunais à LGPD.** [09 Jan. 2021]. Disponível em: https://www.conjur.com.br/2020-dez-16/cnj-aprova-resolucao-padroniza-adequacao-tribunais-lgpd.

LOPES, Everton - **Os impactos da não adequação e a necessidade do Compliance Digital.** [10 Jan. 2021]. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/impactos-da-nao-adequacao-e-compliance-digital.

PUGLIESI, Rodrigo - **A LGPD e seus desafios no setor público.** [12 Jan. 2021]. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-desafios-setor-publico-serpro.

SERPRO – **A LGPD em um giro.** [12 Jan. 2021]. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-giro.

VALENTE, Fernanda - **Tribunais trabalham para mudar a cultura digital interna e adequar à LGPD.** [12 Jan. 2021]. Disponível em: https://www.conjur.com.br/2020-nov-16/tribunais-trabalham-mudar-cultura-interna-adotar-lgpd.

O Rastreamento e Compartilhamento de Dados pessoais e a COVID-19

Márcia Santana Fernandes[130]

RESUMO

O ano de 2020, entra na história da humanidade como o ano da grande pandemia do coronavírus. Esse ano também marca a necessária reafirmação da democracia, dos direitos humanos, dos direitos fundamentais e dos direitos da personalidade. A COVID-19 está sendo reconhecida e estudada; não há tratamento, vacina ou medicamento para o seu enfrentamento. Até 26 de janeiro de 2021, a COVID-19 já contaminou mais de 100 milhões de pessoas, com mais de dois milhões de mortes. As diferentes ações preventivas, de mitigação e resolução para enfrentar a pandemia envolvem medidas desde de imposição de hábitos de higiene, lavagem das mãos, uso de mascaras, testagem e vacinação. Em qualquer uma delas, a utilização de dados pessoais e dados sensíveis são centrais para os estudos epidemiológicos e para o estabelecimento de políticas públicas nacionais e internacionais. Neste contexto, o rastreamento de contato por meio de aplicativos se avolumou em todo mundo e, na mesma proporção, os questionamentos éticos e jurídicos relacionados a garantia dos direitos fundamentais e de personalidade – de privacidade e proteção de dados pessoais. A partir desta constatação, a questão de estudo tem como objetivo refletir sobre o impacto do rastreamento de dados pessoais e a garantia destes direitos para o enfrentamento da COVID-19. O método utilizado é qualitativo, hipotético-dedutivo, de revisão narrativa de literatura em língua Portuguesa e língua Inglesa, em bases de dados indexadas, documentais publicadas e noticias jornalísticas, publicadas por órgãos de impressa e blogs. Em conclusão: A COVID-19 exige ações técnicas, políticas e econômicas para proteger e evitar o alastramento da doença em nível populacional global, entretanto as situações de urgência e emergência para o enfrentamento da pandemia não justificam a supressão indiscriminada, ou mesmo a minimização do direito à privacidade e a proteção de dados pessoais.

PALAVRAS-CHAVE

COVID-19; urgência e emergência; rastreamento de dados pessoais; privacidade e proteção de dados.

[130] Advogada e Consultora na área de Bioética e Saúde e Proteção de Dados Pessoais. É Pos-Doutora pelo Programa de Pós-Graduação de Medicina em Ciências Médicas, da Faculdade de Medicina da UFRGS (2009-2011). Doutora em Direito pela UFRGS, PPG-Faculdade de Direito (2008). Professora e Coordenadora Adjunta do Mestrado Profissional em Pesquisa Clínica do HCPA (2016). É Pesquisadora Associada do Laboratório de Pesquisa em Bioética e Ética na Ciência do Centro de Pesquisas do Hospital de Clínicas de Porto Alegre-LAPEBEC/HCPA e do Comitê de Bioética do HCPA (2002). Professora Colaboradora do PPG/Dir-PUCRS (2018). Professora do Curso de Direito da Universidade Feevale (2018). Research fellow no UZH Digital Society Initiative (2020) - Universidade de Zurique, Suíça. http://lattes.cnpq.br/2132565174726788

Tracking and Sharing of Personal Data and COVID-19

ABSTRACT

The year 2020, will enter into human history as the year of the great coronavirus pandemic. This year also marks the necessary reaffirmation of democracy, human rights, fundamental rights and the personality rights. COVID-19 is being recognized and studied; there is no treatment or medication for coping. As of January 26, 2021, COVID-19 has infected more than 100 million people, with more than two million deaths. The different preventive, mitigation and resolution actions to face the pandemic involve measures ranging from the imposition of hygiene habits, hand washing, the use of masks, testing and vaccination. In any of them, the use of personal data and sensitive data are central to epidemiological studies and to the establishment of national and international public policies. In this context, contact tracking through applications has increased worldwide and, in the same proportion, ethical and legal questions related to the guarantee of fundamental and personality rights - privacy and protection of personal data. Based on this observation, the study question aims to reflect on the impact of tracking personal data and the guarantee of these rights for coping with COVID-19. The method used is qualitative, hypothetical-deductive, of narrative review of literature in Portuguese and English, in indexed databases, published documents and journalistic news, published by print media and blogs. In conclusion: COVID-19 requires technical, political and economic actions to protect and prevent the spread of the disease at the global population level, however the urgent and emergency situations to face the pandemic do not justify the indiscriminate suppression, or even the minimization of right to privacy and protection of personal data.

KEYWORDS

COVID-19; urgency and emergency; tracking of personal data; privacy; data protection.

Introdução

O ano de 2020, entra na história da humanidade como o ano da grande pandemia do coronavírus. Há um ano atrás, em 30 de janeiro de 2020, a Organização Mundial da Saúde (OMS) declarou que a então epidemia constituía uma Emergência de Saúde Pública de Importância Internacional (ESPII), o mais alto nível de alerta de risco sanitário conforme o Regulamento Sanitário Internacional (RSI) e, em 11 de março de 2020, que a situação havia se desenvolvido para uma pandemia. (OMS & OPAS, 2020)

O número de mortos e contaminados no mundo são avassaladores, até o início de fevereiro de 2021, com base nas informações fornecidas pela Universidade de Medicina John Hopkins, a COVID- já contaminou mais de 100 milhões de pessoas, com mais de dois milhões de mortes[131]. As vacinas, estudadas e produzidas em tempo recorde, ampliam as esperanças para a médio e a longo prazo minimizar os efeitos dramáticos desta pandemia, mas nos números têm escalado patamares altos e novas variantes do vírus sendo detectadas em muitos países.

A vacinação de grande parte da população mundial está longe de ocorrer, por isso medidas desde de imposição de hábitos de higiene, lavagem das mãos, uso de mascaras e testagem devem ser mantidas para enfrentar a pandemia. Neste contexto, o rastreamento digital se avolumou em todo mundo e, na mesma proporção, os questionamentos éticos e jurídicos relacionados a garantia dos direitos fundamentais e de personalidade – de privacidade, proteção de dados pessoais e autodeterminação informativa. A partir desta constatação a questão de estudo tem como objetivo refletir sobre o impacto do rastreamento de dados pessoais e a garantia destes direitos para o enfrentamento da COVID-19.

Qualquer pandemia exige ações técnicas, políticas e econômicas para proteger e evitar o alastramento da doença em nível populacional global. E a COVID-19 não é diferente e seu impacto global, durabilidade e efeitos danosos têm sido sentidos, mostrando e agravando desigualdades sociais e precarizando o desenvolvimento econômico e social. Por isso, a realidade exige o enfrentamento da pandemia com a

[131] É importante ressaltar que os dados apresentados pela Organização Mundial da Saúde (OMS), pelo Ministério da Saúde (MS) do Brasil e pelas secretarias da saúde de estados e municípios não são coincidentes, podendo variar para mais ou para menos. Nesse sentido, os dados publicados pela Universidade de Medicina John Hopkins para o Brasil (através do Coronavirus Resource Center, https://coronavirus.jhu.edu/map.html) podem não coincidir com os dados apresentados pelo Ministério da Saúde do Brasil (https://coronavirus.saude.gov.br/).

concretização da solidariedade, da liberdade, do respeito aos seres humanos e às gerações futuras e ao desenvolvimento interplanetário, oportunizando condições concretas para garantir a existência da vida e a proteção do meio ambiente.

É fato que a pandemia da COVID-19 impõe múltiplos desafios e impacta a vida social e privada de todos nós. Inúmeras medidas, em diferentes áreas, são tomadas diariamente para minimizar efeitos negativos à saúde da população, inclusive àqueles originados por chefes de estado negacionistas, que tentam aplacar a seriedade do problema, polarizando e politizando políticas de saúde e desprezo do conhecimento científico.

O enfrentamento da COVID-19 tem navegado em águas turvas e, como em outras partes do mundo, se configura como problemático no Brasil, quanto ao direcionamento articulado, em todo o país, de medidas para manutenção e ampliação do distanciamento social. A situação sanitária fica ainda mais agravada pelas condições sociais, econômicas e políticas do país, que incluem inequalidades sociais, saneamento básico precário para mais 40% da população, o desaparelhamento e o enfraquecimento das universidades e institutos de pesquisa e a educação precária.

O cenário brasileiro para o enfrentamento adequado da pandemia também é agravado pela instabilidade política criada por ações erráticas do governo federal, representado pelo Presidente da República, que em seu discurso, expresso em praça pública e nas mídias sociais, enfraquece a orientação sanitária para o enfrentamento da COVID-19 estabelecida pela Lei Federal 13.979, de 6 de fevereiro de 2020 (Brasil, 2018).

A premissa inerente ao planejamento e à implementação de políticas públicas e ações eficazes e adequadas para enfrentar epidemias, endemias e pandemias é o interesse público, é este perpassa pelo atendimento de expectativas de direito dos cidadãos e a confiança depositada na gestão e prestação de contas estatal e no atendimento dos princípios da moralidade, da finalidade e da transparência. Medidas devem ser projetadas e aplicadas e, em particular, o princípio da confiança deve ser o fio condutor entre Estado e cidadão na obtenção de dados e informações epidemiológicas confiáveis, e, precisamente, neste momento para o enfrentamento da COVID.

Portanto, no cenário pandêmico o objetivo central do compartilhamento de dados pessoais e informações sensíveis é auxiliar no desenvolvimento de pesquisas epidemiológicas, bioestatísticas e experimentais para conhecer a manifestação e os reflexos, presentes e futuros do Coronavírus na saúde humana e planejar políticas públicas de prevenção, assistência e vacinação.

Ao mesmo tempo, deve ser preservada a dignidade da pessoa humana, estabelecida pelos direitos fundamentais e de personalidade, por meio da garantia do direito a privacidade e a proteção de dados pessoas. Assim, o objetivo central deste trabalho é refletir sobre o impacto ético e jurídico do rastreamento de dados pessoais para o enfrentamento da COVID-19, fazendo a seguinte pergunta: como compatibilizar o rastreamento de dados pessoais em situações de urgência e emergência, como a pandemia COVID-19, e o respeito à privacidade e à proteção de dados pessoais?

O método utilizado é qualitativo, hipotético-dedutivo, de revisão narrativa de literatura em língua Portuguesa e língua Inglesa, em bases de dados indexadas, documentais publicadas e noticias jornalísticas, publicadas por órgãos de impressa e blogs.

A hipótese é de que o rastreamento e o compartilhamento de dados pessoais podem colaborar no enfrentamento da COVID-19, mas o sistema de rastreamento implementado e o compartilhamento de dados deve atender aos princípios da finalidade, da necessidade, da segurança e da autodeterminação informativa, em respeito à privacidade e à proteção de dados pessoais.

A hipótese estabelecida neste trabalho considera situações jurídicas de Estados Democráticos de Direito, não abarcam situações de países não democráticos, autoritários ou ditatoriais; isso é considerando aqueles Estados que reconheçam liberdades individuais e fundamentais, os direitos humanos e os direitos de personalidade - destaque a privacidade e a proteção de dados pessoais; expressamente reconhecidos nas Constituições e em leis específicas e no sistema internacional de tratados e convenções internacionais.

O trabalho está estruturado em duas partes: a primeira, trata do rastreamento, suas características, metodologias de funcionamento e utilidade para o enfrentamento da COVID-19 e a segunda, trata da relação entre os sistemas de rastreamento, o interesse público e a garantia do direito fundamental ao livre desenvolvimento da personalidade e ao direito de personalidade inerente à privacidade e à proteção de dados pessoais e dados pessoais sensíveis.[132]

[132] O Regulamento Geral de Proteção de Dados (RGDP) da União Europeia e a Lei Geral de proteção de Dados (LGPD) brasileira tratam destes conceitos de forma semelhante. O conceito legal de dado pessoal é todo aquele relacionado a uma pessoa natural identificada ou identificável e o dado pessoal sensível é aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

PARTE I - A COVID-19 E O RASTREAMENTO DE CONTRATOS E DE DADOS PESSOAIS E SENSÍVEIS: EXEMPLOS DA UNIÃO EUROPEIA E BRASIL

A complexidade e a significância de uma pandemia evidenciam a diversidade do planeta e sua caoticidade, impondo desafios para impedir o alastramento do vírus como medidas preventivas para restringir a circulação de pessoas e distanciamento social - de isolamento, confinamento, quarentena; medidas de higiene e uso de máscaras e rastreamento[133] de contatos e de dados pessoais.

1.1 As medidas preventivas para enfrentamento da COVID-19

O isolamento ocorre em nível individual, quando os indivíduos restringem o contato social voluntariamente ou quando a pessoa infectada é retirada do convívio interpessoal, medida recomendada pela OMS e adotada em muitos países do mundo para redução do avanço do Coronavírus. A quarentena envolve um grupo de pessoas em situação de risco. *A restrição ao acesso às pessoas com presumível exposição à doença contagiosa por um período estabelecido de tempo é a estratégia básica*, no caso da COVID-19, esse período é, em média, de 14 dias. O confinamento é uma medida mais restritiva, pois é imposta coercitivamente a toda população pelas autoridades de saúde. Essa medida, por sua radicalidade, ocorre quando há dificuldade em identificar indivíduos ou grupos de risco. *O confinamento social amplo tem como finalidade a contenção da doença nos limites de uma fronteira epidemiológica.* (Goldim, 2020*)*

As três estratégias de restrição de contato social – o isolamento, a quarentena e o confinamento – estão sendo utilizadas para conter o avanço da COVID-19 têm reflexos significativos econômicos, sociais e de saúde. Assim, outras alternativas devem ser pensadas para utilização conjunta com as três estratégias de restrição de contato social devem ser implementadas, como os cuidados pessoais e higiene, utilização de equipamentos de proteção, como as máscaras e rastreamento de contatos (manual ou digital) – a composição benéfica e positiva do trinômio TRI - *Testar, Rastrear e Isolar* (em inglês *TTI – Test, Trace and Isolate*) (Royal Society, 2020)*[134]*. Todas estas medidas

[133] É importante esclarecer que a palavra "rastreamento" está sendo utilizada em seu sentido genérico, isto é, como ato de acompanhar ou perseguir pistas, e não no sentido epidemiológico, que significa conjunto de exames e testes que se faz em uma população aparentemente sadia ou infectada para descobrir doenças latentes ou em estágio precoce.

[134] A título de curiosidade o prefixo TRI no Rio Grande do Sul, Brasil (Estado no sul do Brasil em que nasci) significa algo positivo, benéfico, bonito ou especial. O trinômio utilizado no sentido epidemiológico foi proposto em inglês TTI – *Test, Trace, Isolate*, no relatório do Royal Society. Ver em Royal Society Report. Success of test, trace and isolate programmes depends on speed, compliance and monitoring, 27 May 2020. Acessado em 02 de fevereiro de 2021, disponível em

devem ser utilizadas em conjunto para desenhar respostas epidemiologicamente compatíveis e cientificamente justificáveis, como por exemplo desenvolvimento de vacinas. No caso da COVID-19, a as pesquisas clínicas para produção de vacinas ocorrem em tempo recorde, de 12 a 14 meses, diferente de situações anteriores que os estudos duravam uma média de 10 anos. (Sharma; Sultan; Ding; Triggle, 2020)

Segundo Anne Johnson, professora de Epidemiologia de Doenças Infecciosas no University College London, vice-presidente da Academia de Ciências Médicas entende que:

> *Todos os aspectos de um sistema coordenado de TTI* (em português TRI) *devem ser firmemente guiados pelo propósito central da saúde pública de reduzir as transmissões e contribuir para manter um número de reprodução efetivo*. *Juntamente com seus benefícios à saúde pública, o sistema permite a identificação de casos para cuidados clínicos e fornece inteligência sobre o curso da epidemia (vigilância)*, *o que, por sua vez, permite que o TTI seja direcionado para otimizar seu propósito principal. Os testes rápidos também permitem que aqueles que não estão infectados, e suas famílias, continuem com suas vidas.* (Royal Society, 2020)

2.2 Do rastreamento de dados pessoais: uma visão da literatura especializada no caso da COVID-19

O rastreamento manual, tradicionalmente utilizado nos casos de doenças infectocontagiosas, envolve a comunicação da pessoa ou das autoridades de saúde ao grupo de pessoas que tiveram contato com as pessoas infectadas, no caso da COVID há indicativos que a comunicação para pessoas não residentes com o infectado pode reduzir a propagação em 5 a 15% (Royal Society, 2020). Além, do rastreamento manual, na área da saúde pública e da epidemiologia, tecnologias de informação, os aplicativos de rastreamento de contato, que envolvem a utilização de algoritmos, inteligência artificial e Big Data, apresentam-se como uma outra alternativa e podem agregaram valor as diversas metodologias utilizadas para análise dos dados, permitindo o nascimento da informação significada, com finalidade direcionada e declarada. (Fernandes, 2019; Fernandes & Goldim, 2020)

Conforme dados publicados por Samuel Woodhams, 47 aplicativos de rastreamento de contatos estão sendo usados em 28 países; medidas alternativas de

https://royalsociety.org/news/2020/05/success-of-test-trace-and-isolate-programmes-depends-on-speed-compliance-and-monitoring/

rastreamento digital estão ativas em 35 países; as tecnologias de vigilância física estão em uso em 11 países; a censura relacionada com a COVID-19 tem sido imposta por 18 governos; e as interrupções da internet continuam em 3 países apesar da pandemia. Woodhams aponta que, dos 47 aplicativos de rastreamento no mundo, rodando em razão da COVID-10, 24 aplicativos (51%) contêm rastreamento do *Google* e do *Facebook*, 11 (23%) não têm política de privacidade; 25 (53%) não revelam por quanto tempo irão armazenar os dados dos usuários; e 28 (60%) não têm medidas de anonimato declaradas publicamente. Esses dados evidenciam que os aplicativos de rastreamento de contatos apresentam riscos à garantia dos direitos de privacidade e à proteção de dados pessoais e sensíveis. (Woodhams, 2020)

A Recomendação da Comissão Europeia EU 2020/518/2020 estabeleceu características e funções para o rastreamento de contatos por aplicativos. Quanto as características são:

> (...) *softwares de aplicação que funcionam em dispositivos inteligentes, nomeadamente telemóveis inteligentes, geralmente concebidos para uma interação abrangente e específica com recursos em linha, que tratam dados de proximidade e outras informações contextuais recolhidas por vários sensores presentes em qualquer dispositivo inteligente, e que são capazes de trocar informações através de várias interfaces de rede com outros dispositivos conectados* (União Europeia, 2020).

A Recomendação EU 2020/518/2020, item 12, indica três funções para implementar as medidas de rastreamento, são elas:

> *i) informar e aconselhar os cidadãos e facilitar a organização do acompanhamento médico de pessoas com sintomas, muitas vezes com a ajuda de um questionário de autodiagnóstico;*
> *ii) alertar as pessoas que tenham estado na proximidade de uma pessoa infectada com o fim de interromper as cadeias de infecção e evitar o ressurgimento de infecções durante a fase de reabertura; e*
> *iii) controlar e obrigar a cumprir a quarentena às pessoas infectadas, eventualmente em combinação com funcionalidades que avaliem o seu estado de saúde durante o período de quarentena.*

A geolocalização, um dos tipos frequentes de rastreamento de dispositivos, que permite, o rastreamento de pessoas e contatos e funciona a partir de coordenadas geográficas. Essas coordenadas são identificadas por meio de tecnologias sem fio, que utilizam emissão de ondas de rádio entre dispositivos, como *wi-fi*, *bluetooth*, GPS e

AGPS. A rede *wi-fi* e o *bluetooth* têm pouco alcance (de apenas alguns metros), já o GPS envolve a triangulação de frequências feita por satélites, que permite a determinação aproximada de coordenadas geográficas. O sistema AGPS consiste na combinação entre o sistema GPS e radiofrequência provida por redes de telefonia, melhorando significativamente a precisão do rastreamento.

Em vista de garantir o equilíbrio entre a utilização de aplicativos de rastreamento para compartilhamento de dados e informações para enfrentamento da COVID-19 e a garantia de direitos fundamentais e da proteção de dados pessoais, a União Europeia, por meio da Recomendação EU 2020/518/2020, sugeriu as seguintes orientações e princípios: 1) salvaguardas de proteção à privacidade, à proteção de dados, aos direitos fundamentais e para estabelecer medidas para prevenir a estigmatização de pessoas afetadas pela COVID-19 e garantir a confidencialidade das comunicações; 2) medidas eficazes e menos intrusivas para utilizar os dados pessoais, anonimizados e agregados; 3) medidas de segurança relativas às tecnologias, a exemplo da encriptação, uso justificado para eventual acesso das autoridades sanitárias; 4) cibersegurança para proteger a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados; 5) prazo condicionado ao final da pandemia e medidas para o descarte dos dados pessoais obtidos com essa finalidade; 6) mecanismos anonimizados de alerta em caso de infecção confirmada e em caso de contato de pessoas com a pessoa infectada, e 7) requisitos para a devida transparência de parâmetros para o resguardo da privacidade, a fim de assegurar a confiança nos aplicativos. (União Europeia, 2020).

Outro ponto a ser considerado, é a precariedade de acessibilidade de aplicativos, em especial para a população idosa acima de 70 anos e menos de 10 anos; a inexatidão da informação e a possível estigmatização de pessoas, em contraste com a motivação de defesa da saúde pública – com relação, tanto ao sistema operacional como ao tipo de aparelho telefônico móvel. (Fernandes & Goldim, 2020)

O uso do rastreamento para o enfrentamento da COVID-19 tem sido tratado pela literatura com possível impacto positivo, apesar das questões éticas e jurídicas relacionadas à garantia da privacidade e da proteção de dados pessoais, desde que esta medida seja integrada com outras estratégias de saúde, sejam elas preventivas -cuidados de higiene, uso de mascarás e de distanciamento social – ou envolvidas em terapêuticas de imunização.

O Editorial do The Lancet Digital Health de novembro de 2020, *Contact tracing: digital health on the frontline,* refere estudos de revisão sistemática de literatura, uma

survey desenvolvida pela Microsoft e estudos de modelagem e simulação envolvendo a utilização de aplicativos para rastreamento de contatos durante a COVID-19. Um ponto comum a todos estes estudos é que o rastreamento de dados é uma ferramenta que pode colaborar no enfrentamento da pandemia desde que seja parte de uma estratégia integrada de saúde. A posição do Editorial é que o rastreamento é imperativo, conjuntamente com apoio financeiro para que as pessoas possam realizar a quarentena (ou serem liberadas da quarentena) e testagem maciça da população para enfrentamento da segunda onda do COVID-19. (The Lancet Digital Health, 2020)

Braithwaite, Callender, Bullock, Aldridge desenvolveram revisão sistemática de literatura de estudos, publicados nas bases indexadas no período de 2000 a 2020, envolvendo rastreamento de contato automático, via aplicativos, semiautomático ou manuais, para controlar a COVID-19, síndromes respiratórias severas, como a MERS – *Middle East Respiratory Syndrome*, influenza e Ebola vírus. Este estudo demonstrou que no caso da COVID-19 é necessário a utilização de rastreamento de contato por um número significativo de pessoas, entre 56% a 95% da população para, potencialmente, reduzir a transmissão do Coronavírus; no entanto, sugerem que estudos empíricos sejam realizados para observar a efetividade, as medidas de cuidado como a equidade e privacidade e sua interação com o rastreamento manual. (Braithwaite; Callender; Bullock; Aldridge, 2020)

2.3. O rastreamento pessoal de dados para enfrentamento da COVID-19: exemplos utilizados na Alemanha, Portugal, Reino Unido e no Brasil

Preliminarmente, é importante esclarecer a motivação da escolha de tratar a experiência da Alemanha, de Portugal, do Reino Unido e do Brasil, nos casos de rastreamento de dados para enfrentamento da COVID-19. A Alemanha foi considerada porque melhor respondeu, de entre os países europeus, à primeira onda da pandemia e utiliza, desde o primeiro semestre de 2020, aplicativo de rastreamento de dados. Portugal teve um enfrentamento razoável na primeira onda da COVID-19, sem a utilização de aplicativos de rastreamento. No entanto, implementou um sistema em razão do aumento significativo de casos, na segunda onda da pandemia, iniciada no segundo semestre de 2020. O Reino Unido é considerado por ter políticas voltadas a digitalização dos serviços públicos de saúde, envolvendo pesquisadores da área e políticas governamentais, dentre as quais uma para o enfrentamento da COVID-19. Por fim, o Brasil, por ser o país natural da autora e, também, por ter a triste marca de ser o segundo pais do mundo com o maior número de

mortos causadas pelo COVID e não ter utilizado aplicativo de rastreamento de dados pessoais.

A Alemanha, conforme mencionado, teve sucesso no controle da pandemia na primeira onda, sendo considerado um dos países que melhor controlou a pandemia. O resultado utilizou um intenso sistema de testagem, rastreamento de contato e quarentena, além dos cuidados de higiene e uso de máscara, conforme Editorial do British Medical Journal (2020). O rastreamento foi realizado pelo aplicativo conectado ao Google, utilizado a partir de julho de 2020, denominado de *Corona-Watn-App,* com funcionamento apenas na Alemanha (Germany, 2020). Este aplicativo foi disponibilizado gratuitamente, via os contatos da companhia telefônica Deutsche Telekom de forma anonimizada e decentralizada. Não havia uma base centralizada de dados, os dados permaneceram apenas no próprio telefone e são deletados após 14 dias. O governo alemão, nem o Instituto Robert Koch (RKI), responsável por ações e estudos na área de saúde pública na Alemanha, ou qualquer pessoa tem acesso a identidade dos dados – medidas para atender ao Regulamento Geral de Proteção de Dados (RGPD). (Deutsche Telekom, 2020)

O propósito do aplicativo alemão *Corona-Watn-App* foi permitir que os dados informados pudessem fornecer ao Instituto Roberto Koch avaliações mais assertivas para conter a disseminação e melhor contenção do Coronavírus, na modelagem de fluxos de movimento – em nível nacional, repartidos em nível estatal e até ao nível distrital-comunitário. (Deutsche Telekom, 2020)

A Alemanha, no entanto, enfrenta dificuldades na segunda onde, iniciada em dezembro de 2020, com o aumento significativo dos números de casos de contaminados contaminados e de mortes.(Universidade de Medicina John Hopkins, 2020)[135] O Governo alemão reconhece que não está conseguindo rastrear 75% dos novos casos e também que o aplicativo de rastreamento, *Corona-Watn-App,* não está tendo a utilidade esperada, pois apenas 60% das pessoas que testaram positivo passaram os seus contatos via o aplicativo, além de outras dificuldades.(CNBC, 2020)

Em Portugal, o rastreio de contato com a finalidade de informar sobre a exposições de risco ao vírus, por meio do aplicativo *Stayaway Covid*. Este aplicativo foi implementado final de 2020, permitindo a monitorização por geolocalização de contatos,

[135] Estes números correspondem ao dia 06 de fevereiro de 2021, data da pesquisa. Para dados atualizados ver em: Universidade de Medicina John Hopkins para o Brasil (através do Coronavirus Resource Center, https://coronavirus.jhu.edu/map.html)

com risco elevado de contágio, com alguém diagnosticado com a COVID-19. A pessoa com teste positivo de Conoravírus informa no aplicativo de forma anônima e esta informação é disparada a todos aqueles que estiveram próximos. Esta informação, potencialmente pode alertar pessoas ainda assintomáticas e de forma preventiva. A participação é voluntária, com garantias de anonimato (com o uso de identificadores aleatórios que não revelam identidades pessoais) e de proteção aos dados pessoais, em razão da legislação nacional e da RGPD. Além disso o código do software desenvolvido para o aplicativo está aberto para conhecimento e o seu uso somente ocorrerá durante a pandemia, ou seja, assim que a pandemia for declarada finda pela Direção Geral de Saúde haverá o término da operação[136]. (Portugal, 2020)

O Reino Unido, hoje não mais parte da União Europeia, tem organizado aplicativos para utilização pelo National Heath Service (NHS). Em relatório conjunto, *Effective Configurations of a Digital Contact Tracing App: A report to NHSX*[137], sobre a efetividade dos aplicativos de rastreamento, pesquisadores do *Pathogen Synamics Group, Big Data Institute, Nuffield Departament of Medicine da Universidade de Oxford, Wellcome Trust Centre for Ethics and the Humanities, faculty. Ai, IBM UK e o UCL/Ala Turning Institute*, estão desenvolvendo um sistema que possa ser seguro e funcional.

O aplicativo tem dois componentes: um tecnológico e outro atendendo a requisitos epidemiológicos. A funcionalidade tem que ser baseada em um algoritmo "transparente" – isso é sua fórmula matemática (1) parece e tem a finalidade epidemiológica; (2) ela foi testada por analise de simulação e sensibilidade e (3) pode ser auditada e otimizada a medida em que os dados sejam disponibilizados e os estudos epidemiológicos se desenvolvam. Este aplicativo tem o objetivo de estabelecer um programa epidemiológico para minimizar, analisar e controlar as condições para saída de situações de *lockdowns* e quarentenas.

---

[136] Stayaway Covid, acessado em 03 de fevereiro de 2021, disponível em em https://stayawaycovid.pt/?cn-reloaded=1 No caso do *Stayway COVID*, o governo português, em razão do aumento dos casos na segunda onda da COVID-19, em setembro querida implementar o uso obrigatório do aplicativo, questão que foi criticada pela Comissão Nacional de Protecção de Dados (CNPD), sugerindo que o uso fosse voluntário como os demais Estados europeus, em respeito a Convenção de Proteção de Dados do Conselho da Europa e a RGPD, além da própria legislação nacional.

[137] NHSK é unidade do governo Britânico, que se reporta diretamente ao Secretário de Estado e ao Chefe Executivo do National Heath Service (NHS) e trabalha próximo ao *Government Digital Service,* para desenvolver políticas e desenvolver boas práticas tecnológicas, de *digital* data, incluindo o compartilhamento de dados na estrutura do NHS. Este grupo reúne especialistas e pesquisadores do *Department of heath and Social Care*; NHS e *NHS Improvement* - médicos, tecnólogos, especialistas em políticas, desenvolvedores, cientistas de dados e gerentes de projetos. Mais detalhes ver em: https://www.nhsx.nhs.uk/about-us/who-we-are/

O relatório apresenta aspectos positivos e de forma simulada. Foi observado um apoio para redução do número de infectados e a liberação de um maior número de pessoas em quarentena. Entretanto, ele sugere que os controles epidemiológicos realizados por meio de aplicativos não devem estar dissociados de intervenções de política públicas de saúde, como a testagem, o distanciamento social e o uso de equipamentos de proteção pessoal. (Hinch; Probert; Nurtay et.al, 2020)

O Brasil utiliza um aplicativo informativo - o *Coronavírus-SUS* - desde julho de 2020, o seu uso é voluntário e a tecnologia de geolocalização é para informar sobre o COVID-19, desenvolvida em parceria do Ministério da Saúde do Brasil, Google e Apple e pode ser utilizado nos sistemas Android ou iOS. O aplicativo não é interativo, mas é, supostamente, informativo - contém informações sobre as Unidades de Saúde próximas ao endereço do usuário e sobre o Coronavírus em geral. Infelizmente, no Brasil as informações fornecidas pelo Ministério da Saúde não são confiáveis. A omissão ou sonegação de dados epidemiológicos por si só, já é grave, ainda mais em meio a uma pandemia. No país, este mascaramento de dados epidemiológicos pelo Ministério da Saúde é inédito e grave. Essa realidade fez com que um consórcio de veículos de imprensa, na mesma época da criação do aplicativo, entre **Folha de São Paulo,** O Estado de São Paulo, Extra, O Globo, G1 e UOL, fosse criado para garantir informação atualizada à população a partir de dados das Secretárias de Saúde dos Estados da Federação, não consolidados pelo Ministério da Saúde.

A ciência brasileira está sob ataque, *SOS Brazil: Science under attack*, pelo atual governo brasileiro, como bem destacou o epidemiologista Pedro C Hallal, na prestigiada revista The Lancet, em janeiro de 2021. (Hallal, 2021) Infelizmente, o governo brasileiro, representado pelo Presidente da República, não mede esforços para desprestigiar dados informações e orientações científicas, começando pelo mascaramento e omissão de dados.

Desde o início da pandemia o Presidente minimiza e nega os efeitos provocados pelo COVID-19 e o seu impacto para a saúde da população brasileira e do planeta; "prescreve" tratamentos prejudiciais, inócuos e não autorizados cientificamente (como a Cloroquina) e, entre outras atitudes, desestimula o programa de vacinação brasileiro e a sua importância para saúde pública. Alias, deve ser dito e reforçado: o Brasil construiu e consolidou, exemplarmente, ao longo de mais de 110 anos, o seu programa de vacinação público, universal e gratuito, amparado por dados científicos e epidemiológicos, hoje em

ataque e em risco de ser desmantelado e o mais agravante, durante uma pandemia sem precedentes no mundo. (Fernandes & Goldim, 2020)

1.4 O rastreamento de dados pessoais por *aplicativos éticos*

Alguns países democráticos adotarem práticas potencialmente lesivas aos direitos fundamentais, por sua inépcia e negligência aos cuidados de saúde pública, assim como expressa pela inadequação do uso de dados – uma ora pela omissão e pelo mascaramento dos dados epidemiológicos e outra pela intenção ou pela coleta de dados pessoais em aplicativos de rastreamento, por meio de sistemas tecnológicos frágeis quanto às salvaguardas de direitos, à eficácia e à segurança, desprezando cuidados com à privacidade e a proteção dos dados pessoais.

Para evitar o mau uso dos aplicativos de rastreamento, Morley, Cowls, Taddeo e Floridi formularam 16 perguntas, aqui apresentadas, de forma sistematizada, em seis (6) aspectos:

1- os dados devem ser imprescindíveis para a proteção efetiva da vida humana;
2- o aplicativo deve ser o melhor método em carácter insubstituível;
3- promover resultados robustos a ponto de afetar medidas de saúde pública distintas;
4- ter tempo determinado para a realização do rastreamento;
5- manter os direitos fundamentais; e da personalidade preservados; e

garantir que o sistema seja seguro, tanto do ponto de vista interno (criptografia e anonimato, por exemplo), como do ponto de vista externo (cibersegurança, por exemplo). (Morley, Cowls, Taddeo e Floridi, 2020)

O estabelecimento de princípios, regras e limites para a implementação de políticas de rastreamento de contato, em razão da pandemia do Coronavírus, é importante desde haja transparência nas proposições, que possibilite a autodeterminação das pessoas em participar ou não, assim como de manter o controle de seus dados e informações.

As intervenções digitais para fornecimento de dados pessoais sensíveis têm um preço, como apontam Morley, Cowls, Taddeo e Floridi (2020). Esse preço está diretamente relacionado à potencial ameaça à privacidade, à igualdade e à justiça. Os aplicativos de rastreamento para a COVID-19 podem servir como instrumentos para criar registros de dados pessoais permanentes e não temporários; interferindo em movimentos e interações sociais e ofuscando a autodeterminação informativa, expondo as pessoas a uma situação incerteza e risco, na qual elas têm pouco ou nenhum controle. Assim, para

os limites serem adequadamente traçados o interesse público deve estar devidamente justificado e a privacidade e a proteção de dados pessoais serem garantidas e respeitadas.

PARTE II- INTERESSE PÚBLICO, PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

É fato que a relação entre o Estado Democrático de Direito e os indivíduos já nasce com o pressuposto do postulado da *supremacia dos interesses da Administração Pública*, que deve pautar sua atuação na obrigatoriedade de princípios constitucionais da *moralidade, impessoalidade e da segurança jurídica*, como ensina Judith Martins-Costa (2015). Vejam como o interesse público se concretiza na situação da COVID-19, atendendo ao necessário respeito aos direitos de privacidade e da proteção de dados.

2.1 O interesse público concretizado na situação de urgência e emergência provocada pela COVID-19

O interesse jurídico deve direcionar ações para perseguir o bem comum. Na situação concreta da pandemia da COVID-19, o interesse público, em primeiro lugar, se apresenta na obrigatoriedade de tomar todas as medidas cientificamente orientadas, para restringir o contato interpessoal, individual ou coletivo, em diferentes níveis de complexidade, como o distanciamento social e o uso de máscaras e em segundo lugar, estabelecer politicas públicas para possibilitar o acesso à vacina e outras tecnologias de saúde pela população.

No que concerne especificamente a coleta, utilização, armazenamento e descarte de dados e informações pessoais têm que ser feito observando duas perspectivas interrelacionadas: a justificativade um interesse público destas atividades e a transmissão adequada do conteúdo desta justificativa para possibilitar a autodeterminação informativa aos interessados e a terceiros. (Cachapuz, 2006)

Michael Ryan, diretor executivo da Organização Mundial da Saúde (OMS) argumenta que o planejamento de coleta de dados e informações são fundamentais para a tomada de decisão, entretanto o cuidado com a qualidade e veracidade das informações devem ser sempre aspectos preliminares à coleta. Conforme suas palavras: *Mesmo com dados, os países podem estar pobres de informações sobre Coronavírus*. […]. Isso significa que o país pode ter uma avalanche de dados, mas estar pobre de informações qualificadas e cientificamente significativas. O que importa, portanto, é ter o número certo dos dados certos, e analisá-los para formular as políticas. (Pinto, 2020)

Assim, o interesse público e sua justificativa está no centro de reflexão no contexto da pandemia e a necessária utilização de dados pessoais e dados pessoais sensíveis. O interesse público na defesa da saúde pública e no combate contra uma crise sanitária em nível global são as motivações e a justificativas plausíveis para o rastreamento de dados pessoais. Neste sentido, em outro trabalho, já tive a oportunidade de defender que o interesse público deve estar sustentado em boa administração e em equilíbrio de interesses privados e coletivos, à luz dos direitos fundamentais e da proporcionalidade. (Fernandes, 2012)

O caráter interdisciplinar e o complexo da noção de interesse público não podem ser olvidados, para analisar situações fáticas e suas repercussões jurídicas. A partir do reconhecimento da realidade deve se estabelecer a composição do conteúdo envolvido no interesse público, sua abrangência e limites. Portanto, assume a noção de interesse público, duas faces: a jurídica e a humanística. (Haeberlin, 2017)

É exigido que o interesse jurídico direcione a sua ação para perseguir o bem comum. Na situação concreta da pandemia da COVID-19, o interesse público, em primeiro lugar, se apresenta na obrigatoriedade de tomar todas as medidas cientificamente orientadas, para *restringir o contato interpessoal, individual ou coletivo, em diferentes níveis de complexidade*, como o distanciamento social e o uso de máscaras e em segundo lugar, estabelecer políticas públicas para possibilitar o acesso à vacina e outras tecnologias de saúde pela população. Em segundo lugar, para melhor atender a população e às pessoas individualmente, a coleta de dados e informações deve ter a finalidade de informar e orientar estudos epidemiológicas, políticas de saúde pública e de vigilância sanitária.

Assim, o reconhecimento dos fatos concretos e urgentes impostos pela COVID-19 exige que o interesse público se apresente na promoção de condições para assistência à saúde, garantindo os direitos fundamentais e de personalidade. O respeito a privacidade, autodeterminação informativa e a proteção de dados, em um cenário de urgência e emergência na área da saúde, como é a situação da COVID-19, são cruciais para estabelecer a linha divisória entre interesse público e o abuso de direitos. Neste contexto, os princípios da publicidade de informações seguras, consolidadas sobre bases científicas, assim como sobre os princípios da moralidade e da transparência, devem pautar e orientar as ações políticas, governamentais e de comunicação geral ao público, como sugerido pela Recomendação EU 2020/518/2020.

2.2 Qualidade do dado coletado e sua amostragem

Além da publicidade de informações seguras as bases que devem pautar o interesse público no combate à pandemia e a para a coleta e uso de dados pessoais, deve estar pautada na qualidade da amostragem e na relevância de dados pessoais coletados, para fundamentar os estudos epidemiológicos de significância, tanto do ponto de vista estatístico, como do ponto de vista ético e de boas práticas científicas.

Portanto, a qualidade da amostragem e a relevância de dados pessoais coletados é fundamenta pesquisas e políticas epidemiológicas necessariamente efetivas e seguras. Nesse sentido, gostaria de apontar a reflexão de Onora O'Neill, que afirma que o acúmulo e a contabilidade de dados não são substitutos para a comunicação com o público em geral, pois os dados ou informações a serem divulgados são pré-selecionadas para amostragem e, de certa forma, a seleção em si pode direcionar a informação e negligenciar uma comunicação genuína, com audiências reais. (O'Neill, 2004)

Na perspectiva filosófica, bioética e jurídica, a confiança é elemento central nas relações humanas, sejam elas interpessoais ou entre os indivíduos com o Estado, envolvendo a confiança nas instituições e nos seus representantes. Entretanto, esse estado de confiança não se apresenta meramente com a divulgação de dados e informações, mas deve ser sustentado sobre uma *narrativa inteligível combinada com uma comunicação genuína nos dois sentidos, para que possa fornecer oportunidades para a verificação e contestação, e possa posicionar, modificar ou recusar a confiança de forma inteligente* para que a expectativa legítima se apresente. (O'Neill, 2004)

O princípio da confiança, articulado com o princípio da boa-fé, deve assegurar as expectativas legítimas para os administrados. A administração estatal deve zelar pelo interesse comum e agir por meio de atos proporcionais e justificáveis, mantendo uma atuação *uniforme e coerente*. *É vedada à Administração a contrariedade desleal* e em desrespeito aos Direitos Fundamentais. A atuação *uniforme, proporcional e coerente* deve ser mantida, mesmo nas situações de urgência e emergência. (Martins-Costa, 2015)

O princípio da confiança está na base das relações jurídicas, sejam de direito público ou privado. Por sua vez, o princípio da proteção da confiança apresenta-se na dimensão individual, ou na vertente *subjetivada* da segurança jurídica. Esse princípio depende do exercício da confiança, com indicação concreta da quebra das expectativas de direito ou com a demonstração clara dos requisitos necessários à sua demonstração – base da confiança, exercício da confiança e frustação da confiança. (Martins-Costa, 2002; Ávila, 2011)

A segurança jurídica, como bem definiu Humberto Ávila, *é uma noção inerente à própria ideia de Direito* e é um princípio que está relacionado diretamente ao princípio do Estado de Direito. O Estado tem a obrigação de oferecer um ambiente mínimo *de certeza, de eficácia e de ausência de arbitrariedade* para que possamos ter de fato um *sistema jurídico*, sustentado pelos princípios da *cognoscibilidade, da confiabilidade e da calculabilidade do ordenamento jurídico.* (Ávila, 2011)

Assim, a natureza do princípio da segurança jurídica esta*, de algum modo,* pautado em *um "direito-garantia", porque a sua realização é prévia ao exercício efetivo de determinados direitos fundamentais* – é pressuposto da atuação do Estado Democrático de Direito. E os direitos fundamentais– *enfatiza-se –servem para que o indivíduo possa exercer a sua autonomia.* (Ávila, 2011)

As expectativas de um ambiente confiável e seguro para o exercício da autonomia é do Estado. Afirma Judith Martins-Costa que o princípio da confiança, justamente, *tem o escopo imediato de assegurar expectativas*. Essas expectativas legitimadas *são como uma confiança objetivada* por uma situação concreta. (Martins-Costa, 2015)

No caso da coleta e uso de dados pessoais para enfrentamento da pandemia e para finalidades precisas, como de assistência à saúde ou previdência, apresenta-se como uma situação de confiança concretizada entre o indivíduo e a administração pública.

Da mesma forma, o Direito Administrativo estabelece como centrais os princípios da expectativa legítima e da motivação *para garantir o cidadão contra o arbítrio estatal,* e eles *devem ser articulados para preservar o pacto social.* O princípio da confiança é preliminar a estes e deve estar ancorado na certeza ou na previsibilidade. *A confiança nas instituições é um pressuposto para o funcionamento da sociedade e estabilidade e de suas instituições.* (Mello, 2006)

A expectativa legítima é do administrado, sendo, portanto, o *resultado de uma série de elementos acidentais,* como o tempo, e a circunstâncias e normas jurídicas relacionadas à ação concreta da Administração. Essa ação é gerada a partir de situações fáticas, com *potencial vinculativo indefinido* prima facie*, variando conforme os elementos acidentais adicionados à confiança*. (Mello, 2006)

O princípio da motivação (a justificação para a coleta e uso de dados pessoais), por sua vez, deve ser percebido, no entanto, a partir da perspectiva do administrador. Ele exige que os atos administrativos, *lato sensu*, assim como os atos políticos, sejam propostos e enunciados por *motivos de fato e de direito*, incluindo a justificação do

processo de tomada de decisão, com narrativa *clara, tempestiva e congruente.* (Mello, 2006)

O interesse público da pesquisa científica, para benefício de toda a comunidade, é a motivação para utilizar dados pessoais. No entanto, a utilização de dados pessoais e dados sensíveis nestas situações, devem, sempre que possível, ser anonimizado, preservado o sigilo, pelas autoridades responsáveis, e de forma consentida. O tratamento de dados pessoais para a realização de estudos por órgão de pesquisa, é, normalmente, expressamente autorizado por leis específicas, como as legislações concernentes à proteção de dados pessoais ou como orientações, expressas em diretrizes internacionais, declarações, regras deontológicas, manuais ou orientação de boas práticas de investigação clínica. (Caldeira, 2020)

Assim ocorre, por exemplo, no Regulamento Geral de Proteção de Dados (RGPD) Europeu, 2016/679, que tem previsão expressa neste sentido em seus considerados 19, 26, 31, 33, 50, 52, 53, 62, 65, 73,88, 113, 129, 156, 157, 159, 160, e em seu Artigos 2º, item 2(d); Artigo 5º , item 1(b) e (e); Artigo 9º, item 2 (j); Artigo 14, item 5 (b); Artigo 17, item 3 (d) e; Artigo 21, item 6; entre outras regras e princípios conectados e a Lei Geral de Proteção de Dados Brasileira, Lei 13.709/2018, que também apresenta dispositivos semelhantes, nos seu Artigo 4º, inciso d; Artigo 5º, inciso XVIII e Artigo 7º, inciso IV. (União Europeia, 2018)

No entanto, a coleta de dados pessoais para investigações científicas deve estar pautada no respeito ao princípio da dignidade humana e no direito ao livre desenvolvimento da personalidade.

2.3. A Privacidade e a proteção de dados pessoais

A proteção à privacidade e à proteção de dados pessoais estão estruturadas no direito geral de personalidade e que, por sua vez, é consequência do direito ao livre desenvolvimento da personalidade. Ambos visam a tutela de aspectos da pessoa humana, entretanto não são sinônimos: o direito ao livre desenvolvimento da personalidade é um direito fundamental, consagrado nas Constituições democráticas, contendo múltiplas dimensões alicerçadas no princípio da dignidade da pessoa humana e o direito geral de personalidade está relacionado e é aplicável nas relações jurídico-privadas. (Mota Pinto, 2018)

O direito fundamental ao livre desenvolvimento da personalidade, há muito reconhecido pela Alemanha e por Portugal, amplia o escopo interpretativo no que concerne à defesa dos direitos da personalidade e o reconhecimento de situações jurídicas

existenciais nele envolvidas, dentre as quais o direito à privacidade e a proteção de dados pessoais são centrais.(Strömholm, 1967).[138] Igualmente, na perspectiva internacional, o reconhecimento da privacidade e da proteção de dados pessoais como direitos humanos, devidamente reconhecidos em tratados e convenções internacionais, portanto como menciona Sarlet são *direitos constitucionais de múltiplos níveis* que demandam um *regulação que transcenda as fronteiras territoriais* com *influência recíproca entre ordens jurídicas*. (Sarlet, 2021)

A privacidade no Direito germânico, em particular após a Segunda Guerra, assumiu um dos tópicos de destaque. A privacidade é protegida como um direito geral de personalidade, expresso no art. 2.1, combinado com o art. 1.1 da Lei Fundamental alemã (*Grundgesetz*) – em outras palavras, a liberdade ao pleno desenvolvimento da personalidade deve ser respeitada em consideração à dignidade humana (Bundesverfassungsgericht, 1957). Esta norma foi interpretada pela jurisprudência da Corte Constitucional Alemã, no caso precedente, *Elfes,* em 1957[139]. Este caso envolvia o reconhecimento de liberdade de atuação de uma pessoa *àquelas atuações que se revistam de particular relevância para o desenvolvimento da personalidade ou ao "núcleo mais próximo da personalidade"*. (Mota Pinto, 2018)

Da mesma forma, este caso determinou que "o direito geral de liberdade de ação" (liberdade física, de expressão, de criação, etc.) somente poderia ser limitado para manter a ordem pública, os bons costumes, a moralidade e direitos de terceiros. (Eberle, 1997; Mota Pinto, 2018)

---

[138] STRÖMHOLM. *Right of privacy and rights of the personality:* a comparative survey. Stockholm: Norstedt & Söners Förlag, 1967. A Alemanha é responsável por uma construção teórica do direito à privacidade como direito da personalidade, construção doutrinária que remonta ao século XIX. Em particular a partir de 1890 muitas monografias foram desenvolvidas tratando dos direitos das pessoas – logicamente aplicadas após a Segunda Guerra Mundial. Três pioneiros para essa construção doutrinária, nos anos 1800 devem ser citados: Otto von Gierke, Karl Gareis e Josef Kohler. Gierke, "inventor" dos direitos gerais de personalidade, postula que se deve integrar uma série de direitos relacionados ao desenvolvimento das pessoas individualmente. Gareis defende a liberdade das pessoas de cuidar dos seus próprios interesses, assim como entende que deve haver o direito ao nome e a honra. Kohler teve um papel de muito destaque na construção dos direitos da personalidade na legislação germânica, seus primeiros estudos foram realizados ainda na década de 1880.

[139] *Elfes case,* Judgment of January 16, 1957 - 1 BvR 253/56, acessado em 05 de fevereiro de 2021, disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1957/01/rs19570116_1bvr025356.html. São os termos da decisão para conceitual livre desenvolvimento da personalidade: 2.a)With the "free development of personality", the Basic Law can not only have meant the development within that core area of personality that defines the essence of man as a spiritual and moral person; for it would be incomprehensible how the development within this core area could violate the moral law, the rights of others or even the constitutional order of a free democracy. It is precisely these restrictions imposed on the individual as a member of the community that rather show that the Basic Law in Article 2, Paragraph 1 of the Basic Law means freedom of action in the broadest sense.

Assim, o direito geral de personalidade apresenta-se em duas dimensões constitucionalmente amparadas como direito fundamental: a primeira relacionada a tutela da individualidade e a segunda protetora da *liberdade de ação pessoal,* que consagra um *direito geral de liberdade*. A estas duas dimensões, no entanto, a doutrina acresce uma terceira dimensão, a denominada dimensão objetiva dos direitos fundamentais, isso é a *eficácia de irradiação* destes direitos em toda ordem jurídica. (Bundesverfassungsgericht, 1958[140]; Mota Pinto, 2018[141])

Igualmente a Alemanha é percursora, na proteção aos dados pessoais e no reconhecimento da autodeterminação informativa como um direito fundamental e humano. A primeira legislação específica no mundo a proteção de dados pessoais foi a Lei Federal de Proteção de Dados, de 1977 e em vigor em 1979. Esta Lei foi originada a partir da Lei de Proteção de Dados do Estado de Hesse e tinha o objetivo de estabelecer limites e garantir a que a finalidade e organização de base de dados foi comunicada claramente à população. Em 1983, o Tribunal Constitucional Alemão reconhece o direito fundamental a autodeterminação informativa, a partir do notório caso do Censo[142].(Bundesverfassungsgericht, 1983; Gasiola, 2019; Sarlet, 2021)

---

[140] O caso *Lüth* trata da proibição da Corte de Hamburgo ao Sr. Lüth de fazer campanha de boicote a exibição do filme *Immortal Beloved* (1951), em razão do diretor do filme Veit Harlan ter sido responsável pelo filme antissemita *Jud Süß* (1940), que, aliás, é considerado o filme mais antissemita de todos os tempos e o mais notórios dos filmes utilizados pelo governo nazista, assistido por mais 20 milhões de expectadores. A proibição da Corte de Hamburgo foi questiona da Corte Constitucional que entendeu que o boicoite do filme por Lüth não caracteriza violação dos bons costumes, estabelecidos no artigo §826 do BGB, e estaria justificado pela Lei Fundamental (*Grundgesetz)* como exercício da liberdade de expressão, um dos direitos mais nobres e que se apresenta como expressão direta da personalidade humana. Portanto, a personalidade humana e a sua dignidade, que livremente se desenvolvem na comunidade, devem ser aplicadas para todas as áreas do ordenamento jurídico, pois há *radiação de efeitos dos direitos fundamentais* na legislação civil. Bundesverfassungsgericht (BVerfG), Lüth Case of the First Senate of January 15, 1958- 1 BvR 400/51 – acessado em 06 de fevereiro 2021, diponível em https://www.servat.unibe.ch/dfr/bv007198.html#208

[141] MOTA PINTO, Paulo. Direitos de personalidade e Direitos Fundamentais – Estudos. Coimbra: Gestual, 2018. Nas palavras de Mota Pinto, nasce na doutrina alemã a partir da decisão do também notório caso *Lüth*: *Integrando esta dimensão objetiva dos direitos fundamentais, distingue-se, assim, na doutrina alemã, desde a decisão do caso Lüth, antes de mais, a sua eficácia de irradiação ("Ausstrahlungswirkung") para toda a ordem jurídica, e, em especial, em relação as entidades privadas.*

[142]O notório caso do Censo decidido em 1983, Corte Constitucional da Alemanha (Bundesverfassungsgericht) *"julgou nulo os dispositivos relacionados à comparação e à transmissão* dos dados para repartições públicas". A Corte alemã reconheceu, neste caso, o direito do cidadão negar informações de caráter pessoal, entendendo como uma faculdade individual consentir, ou não, na coleta, no armazenamento e no compartilhamento de dados pessoais – reconhecendo o direito da autodeterminação informativa, reconhecendo, portanto, que a organização de base de dados pessoais devem ter procedimentos e cuidados adicionais. Ainda este caso decidiu que a transferência de dados científicos é compatível com o direito geral de personalidade, desde que os dados sejam anonimizados, conforme determina a Lei Fundamental. Bundesverfassungsgericht (BVerfG), judgment of December 15, 1983 - 1 BvR 209/83, 1

Em Portugal, por sua vez, o reconhece aos direitos de personalidade, a integridade física ou moral dos indivíduos, coibindo a sua ofensa, expressamente no Código Civil de 1966, em seu artigo 70º, n.º1. A voz corrente e majoritária da doutrina e da jurisprudência portuguesa, como afirma Mota Pinto, entende que a *intenção de consagrar um direito geral de personalidade* é que estava pautada no Direito Civil, pois havia a rejeição *do numerus clauses* para identificar estes direitos. Ainda, o reconhecimento dos direitos de personalidade, anteriormente ao reconhecimento expresso do direito ao livre desenvolvimento da personalidade, na Constituição Portuguesa, revisão de 1997, consolida e consagra o seu reconhecimento. (Mota Pinto, 2018)

Nesta esteira, também Portugal em 1998, reconhece a proteção de dados como um direito fundamental de personalidade, primeiramente na Lei de Proteção de Dados, nº. 67/1998, revogada pela Lei nº. 58/2019. Os alicerces estão no princípio da dignidade da pessoa humana e no dever do Estado em promover medidas para a proteção do cidadão, que sejam ajustados à realidade internacional. Portugal, como país integrante da União Europeia, também está justificando ao Regulamento Geral de Proteção de Dados (RGPD) Europeu, publicado em 27 de abril de 2016. (União Europeia, 2016; Caldeira, 2020)

No contexto brasileiro, por sua vez, não há expressamente o reconhecimento do direito ao livre desenvolvimento da personalidade na Constituição ou mesmo o direito geral de personalidade no Código Civil. Entretanto, a privacidade e a intimidade são direitos fundamental, garantidos constitucionalmente no sistema jurídico nacional, alicerçado na proteção da pessoa humana e sua dignidade.

A Constituição da República Federativa do Brasil (CRFB), Artigo 5º, inciso X, proíbe a violação desse direito, sob pena de indenização por perdas e danos; integrando o suporte fático desse inciso à intimidade e à honra. Esse mesmo artigo inclui a imagem da pessoa como sendo inviolável. O Artigo 5º garante o espaço da casa como *asilo inviolável do indivíduo* (inciso XI); proíbe a interceptação de comunicações telefônicas, telegráficas ou de dados e manifestação escrita (inciso XII); e protege os direitos autorais (incisos XXVII e XXVIII). A CFRB estabelece a ação de *habeas data* (Art. 5º, inciso LXXII), como remédio e forma de garantir o acesso e a retificação de dados pessoais (Brasil, 1988; Sarlet & Keinert, 2015).

Por sua vez, o Código Civil (Lei 10.406/2002) regula, em sua parte geral, capítulo

BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, acessado em 06 de fevereiro de 2021, disponível em https://openjur.de/u/268440.html

II, artigos 11º a 21º, em particular, o direito à privacidade, que é considerado um núcleo essencial aos direitos da personalidade e está positivado no Artigo 21º: *A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.* (Brasil, 2002)

Na sequência, a legislação brasileira com ênfase no Direito Digital[143] inicia com a Lei no 12.965/2014, apelidada de Marco Civil da Internet e se consolida com a LGPD e para a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018. É relevante mencionar também os fundamentos a LGPD, traduz o espírito do tempo[144] em prol da necessária proteção dos dados pessoais como um direito fundamental, embasado pelo direito geral de personalidade humana e pelo princípio do pleno desenvolvimento de personalidade. (Mota Pinto, 2018) A LGPD, em sete incisos do Artigo 2º, contempla: o respeito à privacidade (Inciso I); a autodeterminação informativa (Inciso II); a liberdade de expressão, de informação, de comunicação e de opinião (Inciso III); a inviolabilidade da intimidade, da honra e da imagem (Inciso IV); o desenvolvimento econômico, tecnológico e de inovação (Inciso V); a livre iniciativa, a livre concorrência e a defesa do consumidor; e preconiza *o respeito aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais* (Inciso VII).

No Direito brasileiro, como aponta Ingo Sarlet, a proteção de dados pessoais é um direito fundamental *implícito na Constituição de 1988* e espera-se que a proposta de Emenda Constitucional 17/2019 possa expressamente reconhecer este direito. A importância deste reconhecimento, como destaca o autor, *cobre um espaço próprio e autônomo de incidência,* apesar de ter zonas de convergência com outros direitos, como os direitos à privacidade e a intimidade. (Sarlet, 2021)

---

[143] Expressão de HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital – Transformação Digital, desafios para o Direito. Rio de Janeiro: Editora Forense, 2020.

[144] Em diversos países do mundo à proteção de dados pessoais é regulada. Dos 194 países do mundo, 132, o que corresponde a 66%, têm leis específicas para proteção de dados pessoais e privacidade e 19, o que corresponde a 10%, estão desenvolvendo normas nesse sentido, conforme dados da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD)[144], conselho intergovernamental permanente da ONU. Esses dados, atualizados em 02 de abril de 2020, espelham a importância do tema e da sua respectiva proteção. São exemplos a legislação da União Europeia, mais especificamente o Regulamento de Proteção de Dados (RGPD) 2016/679. UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT – UNCTAD. Data Protection and Privacy legislation Worldwide. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Acessado em 13 de junho de 2020.

O Supremo Tribunal Federal do Brasil, em decisão monocrática, divulgada em 27 de abril de 2020, a Ministra Rosa Weber, em resposta Medida Provisória (MPV) 954/2020, hoje revogada, determinou a suspensão da MPV 954/2020, ordenando que o Instituto Brasileiro de Geografia e Estatística (IBGE) se abstivesse de requerer dados pessoais originados das operadoras de telefonias, sem o consentimento dos seus clientes. Essa decisão é muito significativa, destaco dois aspectos: a decisão barrou a inconstitucionalidade flagrante ao direito fundamental à privacidade e reconheceu em sua interpretação o direito fundamental à proteção de dados pessoais. É importante destacar que a Lei n. 13.709, de 14 de agosto de 2018, contempla o princípio do pleno desenvolvimento da personalidade e da autodeterminação informativa, ou o direito à *autodeterminação informacional* (*the right to informational self-determination*). (Supremo Tribunal Federal do Brasil, 2020)

A autodeterminação informativa é princípio basilar nas legislações relacionadas a proteção de dados pessoais, sendo o exercício da autonomia da pessoa natural o fundamento central, como RGPD. (Döhmann, 2021)

Neste mesmo sentido, outras legislações no mundo, com a brasileira, Lei Geral de Proteção de Dados (LGPD), Lei 13.709 de 14 de agosto de 2018, que expressamente reconhece o direito fundamental a proteção de dados pessoais e a autodeterminação informativa. O direito da autodeterminação informativa contempla dois aspectos importantes, o primeiro, busca resguardar a esfera privada para evitar interferências indesejadas e o segundo, envolve a garantia da participação democrática dos indivíduos, sem vieses, para garantir uma comunicação livre e democrática. (Rouvroy &Poullet, 2009; Fernandes, 2019)

Particularmente, os limites ao rastreamento de dados pessoais em razão da pandemia provocada pelo Coronavírus, devem ser traçados sob o binômio do interesse público e a garantia ao direito geral de personalidade de forma complementar e não dicotômica, tendo o Estado o dever de proteger o cidadão como preceito constitucional. Como afirma Mota Pinto (2018): *A base dogmática para estes deveres de proteção encontra-se, antes, no encargo do Estado consistente na promoção da segurança dos cidadãos, em ligação ao reconhecimento do direito fundamental e com o monopólio estatal do uso da força, caracterizador do Estado de Direito.*

A segurança jurídica, portanto, deve ser a base de fundamentação para justificar o interesse público para realização, por parte do Estado, do rastreamento de dados pessoais para o enfrentamento da COVID-19, atendendo ao princípio da confiança e as legítimas

expectativas dos cidadãos. Quais são estas legítimas expectativas: a utilização de dados pessoais para uso científico, atendendo aos ditames legais (expressos na RGPD e LGPD[145]), a começar pela anonimização dos dados pessoais com segurança; coleta no limite necessário e em respeito da finalidade de promover a saúde pública. Ainda, manter sistemas abertos, para conhecimento dos cidadãos, de sua operabilidade de rastreamento, tempo de armazenamento e formas de descarte das informações previamente coletadas, possibilitando a auditoria de algoritmos. Estes deveres, na mesma proporção e responsabilidade, devem ser *irradiados* para a atuação de empresas de direito privado, colaboradoras na elaboração e funcionamento dos respectivos aplicativos de rastreamento – como a Google e a Apple.

A flexibilização no compartilhamento de dados pessoais em desacerto ao interesse público, no contexto de urgência e emergência, poderá gerar uma situação de *slippery slope*, como defendi.(Fernandes, 2020) No caso do rastreamento dos dados para enfrentamento da COVID-19, as situações de *slippery slope* são aquelas que envolvem uma cadeia de ações e eventos justificáveis, inicialmente, por razões de saúde pública e de interesse público, como os aplicativos que coletam informação por geolocalização, mas, podem evoluir para ações e práticas violadoras do direito geral de personalidade, como vigilância estatal e o controle.(Fernandes & Goldim, 2020)

As situações de urgência e emergência não justificam, a supressão indiscriminada e injustificada do direito ao livre desenvolvimento da personalidade, ou mesmo a minimização de direitos humanos. Ao contrário, o poder de discricionariedade da administração pública não é absoluto e, obrigatoriamente, deve estar justificado nos princípios da finalidade, da moralidade e da transparência para realizar suas ações e usar o seu poder.

3. Considerações finais

O limite para o compartilhamento de dados pessoais em situações de urgência e emergência, como a pandemia da COVID-19, devem estar amparadas em justificativas objetivas, temporalmente fixadas e cientificamente embasadas, para estabelecer o equilíbrio entre o interesse público e o interesse particular.

As diversas circunstâncias e situações envolvidas na COVID-19, e os direitos envolvidos na proteção dos direitos de penalidade, evidenciam que certa flexibilização do

[145] Ver neste artigo item 2.1.

limite do compartilhamento de dados pessoais é justificável em situações de pesquisa epidemiológicas e de pesquisas clínicas para o desenvolvimento de tecnologias em saúde, como medicamentos e vacinas, e para a assistência à saúde. Essas situações são amparadas por regras de direito, deontológicas e de boas práticas e estão submetidas ao escrutínio da comunidade científica, dos comitês de ética em pesquisa, dos órgãos de classe profissionais e são regularmente consentidas.

O cenário que deve ser evitado é o rastreamento de contatos não apresentar de forma clara e tecnologicamente segura as suas finalidades para o uso, armazenamento e compartilhamento de dados pessoais, no presente e no futuro. O interesse público deve ser primordial, agindo em defesa da saúde pública para o enfrentamento da COVID-19. No entanto, não pode servir como justificativa para ofensa ao direito fundamental do livre desenvolvimento da personalidade, tais como o controle injustiçado, a vigilância de seres humanos e o uso futuro dos dados, sem autorização expressa dos usuários.

As políticas públicas responsáveis para lidar com o enfrentamento da COVID-19, devem conjugar medidas eficazes, ou seja, estratégias de restrição de contato social; cuidados pessoais e higiene, utilização de equipamentos de proteção, como as máscaras e rastreamento de contatos, focando no TRI - *Testar, Rastrear e Isolar*.

Estudos de eficácia dos aplicativos de rastreamento da COVID-19, apresentados pela literatura, demonstram que não apresentam a eficácia esperada, ao contrário, apresentam fragilidades técnicas e éticas. Porém, podem corresponder a ações complementares dentre outras medidas coordenadas de saúde pública. Além disso, estes *aplicativos* têm que ser *éticos*, isso é ter sua configuração aberta aos usuários; políticas de privacidade e proteção de dados passíveis de auditorias e melhoramentos constantes; tempo restrito à finalidade de enfrentamento à COVID-19; coleta de dados no limite necessário à finalidade; estruturação de base de dados decentralizada, sem possibilidade de manutenção destas bases para outras finalidades não autorizadas e a utilização voluntária pelos usuários, entre outros cuidados.

Por fim, entendo que a hipótese proposta neste estudo, de que o rastreamento e o compartilhamento de dados pessoais podem colaborar no enfrentamento da COVID-19 é positivo e se confirma, mas para isso é imprescindível que o sistema de rastreamento implementado e o compartilhamento de dados deve atender aos princípios da finalidade, da necessidade, da segurança e da autodeterminação informativa, em respeito à privacidade e à proteção de dados pessoais. o rastreamento de contato não pode ser dissociado das demais medidas de saúde pública para o enfrentamento da COVID-19. A

utilização de tecnologias de informação e comunicação, como os aplicativos de rastreamento, podem ser *instrumentos de agregação e difusão da informação,* desde que utilizada em respeito aos princípios da finalidade, da necessidade e da confiança para *ampliar os horizontes do conhecimento científico, reflexivo e experimentado*[146].

4. Referências bibliográficas

ÁVILA, Humberto. Segurança Jurídica. Entre permanência, mudança e realização no Direito Tributário. Pag. 364-365; São Paulo: Editora Malheiros, 2011.

BRAITHWAITE, ISOBEL; CALLENDER, THOMAS; BULLOCK, MIRIAM; ALDRIDGE, ROBERT W..Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19, *Lancet Digital Health* 2020; 2: e607–21, Published Online August 19, 2020, https://doi.org/10.1016/ S2589-7500(20)30184-9. Acessado em 01 de fevereiro de 2021 e disponível em https://www.thelancet.com/action/showPdf?pii=S2589-7500%2820%2930184-9

BRASIL, Código Civil Brasileiro. Lei 10.406/2002, Brasilia, 2002.

BRASIL, Marco Civil da Internet. Lei 12.965 de 23 de abril de 2014, Brasília, 2014.

BRASIL. Constituição Da Republica Federativa Do Brasil. Brasilia, 1988.

BRASIL. Lei Geral de Proteção de Dados Brasileira (LGPD), Lei 13.709/2018, disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

BRASIL. MINISTÉRIO DA SAÚDE, https://covid.saude.gov.br/. Para o aplicativo acesso em https://play.google.com/store/apps/details?id=br.gov.datasus.guardioes&hl=en&gl=US

BUNDESVERFASSUNGSGERICHT (BVERFG), judgment of December 15, 1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, acessado em 06 de fevereiro de 2021, disponível em https://openjur.de/u/268440.html

BUNDESVERFASSUNGSGERICHT (BVERFG), Lüth Case of the First Senate of January 15, 1958- 1 BvR 400/51 – acessado em 06 de fevereiro 2021, diponível em https://www.servat.unibe.ch/dfr/bv007198.html#208

CACHAPUZ, Maria Claudia. Intimidade e Vida Privada no Novo Código Civil Brasileiro – Uma leitura orientada no Discurso Jurídico, Porto Alegre: Sergio Antonio Fabris Editor, 2006.

CADEIRA, Cristina. A Proteção de dados pessoais, a investigação científica e as transferências internacionais: os códigos de conduta e procedimentos de certificação, in Direito da Sociedade do Conhecimento – Vol. I Estudos na Área do Direito, org. Caldeira, Cristina. Lisboa: Universidade Europeia, Privacy and Data Protection, 2020. E-book acessado em 03 de fevereiro de 2021, disponível em:
https://bo.europeia.pt/content/files/direito_da_sociedade_do_conhecimento-compactado.pdf

CALDEIRA, Cristina; FERNANDES, Márcia S. A partilha de dados pessoais sensíveis, dados epidemiológicos (COVID-19) e genéticos: aspectos jurídicos e bioéticos na perspectiva da União

[146]Texto desenvolvido com base no pensamento de MITTELSTRASS, J. The Loss of Knowledge in the Information Age', in *From Information to Knowledge, from Knowledge to Wisdom: Challenges and Changes Facing Higher Education in the Digital Age*. London: Portland Press, 2010.

Europeia, Portugal e Brasil, in Direito da Sociedade do Conhecimento – Vol. I Estudos na Área do Direito, org. Caldeira, Cristina. Lisboa: Universidade Europeia, Privacy and Data Protection, 2020. E-book acessado em 03 de fevereiro de 2021, disponível em https://bo.europeia.pt/content/files/direito_da_sociedade_do_conhecimento-compactado.pdf

CNBC -HEALTH AND SCIENCE. Why Germany's coronavirus strategy doesn't appear to be working this time around. Acessado em 02 de fevereiro de 2021 e disponível em: https://www.cnbc.com/2020/11/06/why-germanys-coronavirus-strategy-doesnt-appear-to-be-working.html

DEUTSCHE TELEKOM. Telekom teilt Daten über "Bewegungsströme" von Handynutzern mit RKI. 18/03/2020, Acessado em 21 de junho de 2020.

DÖHMANN, Indra Spiecker. A Proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados na União Europeia, *in* Tratado de Proteção de Dados Pessoais, coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

EBERLE, Edward J., Human Dignity, Privacy, and Personality in German and American Constitutional Law. Utah L. Rev. 963. 1997. Acessado em 04 de fevereiro de 2021, disponível em https://docs.rwu.edu/cgi/viewcontent.cgi?article=1067&context=law_fac_fs

BUNDESVERFASSUNGSGERICHT(BVERFG), *Elfes case,* Judgment of January 16, 1957 - 1 BvR 253/56, acessado em 05 de fevereiro de 2021, disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1957/01/rs19570116_1bvr025356.html.

FERNANDES, M. S. Privacidade, sociedade da informação e Big Data. In: Giovana Benetti; André Rodrigues Corrêa; Márcia Santana Fernandes; Guilherme Monteiro Nitschke; Mariana Pargendler; Laura Beck Varela. (Org.). Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa. 1ed.Rio de Janeiro: GZ Editora, 2019, v. 1, p. 182-210.

FERNANDES, Márcia S.; GOLDIM, José Roberto. A integridade na ciência e a COVID-19: o caso da utilização da hidroxicloroquina ou cloroquina, *in* Bioethics & Neuroethics *in* Global Pandemic Times, org. Tauchen, J.; CASTANHEIRAS, N.; OLIVEIRA, N., Porto Alegre: Editora Fundação Fênix, 2020. https://doi.org/10.36592/9786587424538, disponível em https://891aac48-381e-4192-adf5-96afc8de6326.filesusr.com/ugd/9b34d5_bcbaa567ebd64b689e408b454054791d.pdf

FERNANDES, Márcia S.; GOLDIM, José Roberto. Personal Data and COVID-19, *in* Medicine and Ethics in Times of Corona, Eds. Woesler, Martin; Sass, Hans-Martin. Zurich: Lit Verlang, 2020.

FERNANDES, Márcia S.. Slippery Slope: The Tracking of Personal Data and Covid-19, *in* Bioethics & Neuroethics in Global Pandemic Times, org. Tauchen, J.; CASTANHEIRAS, N.; OLIVEIRA, N., Porto Alegre: Editora Fundação Fênix, 2020. https://doi.org/10.36592/9786587424538, disponível em https://891aac48-381e-4192-adf5-96afc8de6326.filesusr.com/ugd/9b34d5_bcbaa567ebd64b689e408b454054791d.pdf

FERNANDES, Márcia. S..Bioética, Medicina e Direito de Propriedade Intelectual. Pág. 169;170. São Paulo: Editora Saraiva, 2012

FOLHA DE SÃO PAULO. Brasil passa de 58 mil mortos por Covid-19, mostra consórcio de imprensa. Folha de São Paulo, 29 de junho de 2020. Acessível em: https://www1.folha.uol.com.br/equilibrioesaude/2020/06/brasil-tem-727-novas-mortes-por-covid-19-mostra-consorcio-de-imprensa.shtml

GASIOLA, Gustavo G.. Criação e desenvolvimento da proteção de dados na Alemanha. JOTA, Opinião e Análise, 29 de maio de 2019. Acessado em 05 de fevereiro de 2021, disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019

GERMANY, *Basic Law for Federal Republic of Germany.* Disponível em: <https://www.btg-bestellservice.de/pdf/80201000.pdf>.

GERMANY.CORONA-WARN-APP:
https://play.google.com/store/apps/details?id=de.rki.coronawarnapp&hl=en&gl=US

GOLDIM, José Roberto. COVID-19, Isolamento, Quarentena e Confinamento. Bioética Complexa e COVID-19. Acessível em https://bioeticacomplexa.blogspot.com/2020/02/,

HAEBERLIN, M. P. Critica da razão do Estado: uma (re)formulação do conceito de interesse público e a correlata construção de um Estado meritocrático de Direito. Pontifícia Universidade Católica do Rio Grande do Sul. Item 33.2 Proposições de tese. Tese de Doutorado. 2014.

HALLAL, PEDRO C. SOS Brazil: Science under attack. The Lancet, Correspondence, publicada em 22 de janeiro de 2021. Acessado em 04 de fevereiro de 2021, disponível em: http://www.thelancet.com/

HINCH, ROBERT; PROBERT,WILL; NURTAY, ANEL ET.AL., *Effective Configurations of a Digital Contact Tracing App: A report to NHSX, April 2020. Acessado em 01 de fevereiro de 2021, disponível em:*
https://cdn.theconversation.com/static_files/files/1009/Report__Effective_App_Configurations.pdf?1587531217

HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital – Transformação Digital, desafios para o Direito. Rio de Janeiro: Editora Forense, 2020.

MARTINS-COSTA, J.. A Boa-Fé no Direito Privado – critérios para sua aplicação. Paulo: Marcial Pons, 2015.

MARTINS-COSTA. Judith. A proteção da legítima Confiança nas Relações Obrigacionais entre a Administração e os Particulares. Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, UFRGS, Porto Alegre, n.22, pp.228-255, 2002.

MELLO, Eduardo Brigidi. O Princípio da Expectativa Legítima e a exposição de motivos das Medidas Provisórias. Revista Tributária e de Finanças Públicas, vol. 66, pp.173-198, Jan-Fev, 2006.

MITTELSTRASS, J. The Loss of Knowledge in the Information Age', in *From Information to Knowledge, from Knowledge to Wisdom: Challenges and Changes Facing Higher Education in the Digital Age*. London: Portland Press, 2010.

MORLEY, Jessica; COWLS, Josh; TADDEO, Mariarosario e FLORIDI, Luciano. *Ethical guidelines for COVID-19 tracing apps.Comment, 28 May 2020,in* https://www.nature.com/articles/d41586-020-01578-0.

MOTA PINTO, Paulo. Direitos de personalidade e Direitos Fundamentais – Estudos. Coimbra: Gestual, 2018.

O'NEILL, Onora. Accountability, trust and informed consent in medical practice and research. Clinical Medicine, Vol. 4, nº 3, May/June,2004.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS) e Organização Pan Americana de Saúde (OPAS) - Regulamento Sanitário Internacional (RSI), Acessível em: https://www.paho.org/bra/index.php?option=com_content&view=article&id=6101:covid19&Itemid=875

PINTO, Ana Estela de Souza. "O país pode ter uma avalanche de dados, mas estar pobre de informações, Folha de São Paulo, 11 de abril de 2020. Acessível em: https://www1.folha.uol.com.br/equilibrioesaude/2020/04/mesmo-com-dados-pais-pode-estar-pobre-de-informacoes-sobre-coronavirus-diz-diretor-da-oms.shtml

PORTUGAL. STAYAWAY COVID, acessado em 03 de fevereiro de 2021, disponível em em https://stayawaycovid.pt/?cn-reloaded=1

ROUVROY, Antoinette and POULLET, Yves. The Right to Informational Self-Determination and *Data Protection?* Dordrecht: Springer Netherlands, 2009, pp. 45–76 <http://dx.doi.org/10.1007/978-1-4020-9498-9_2>.the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in *Reinventing*

ROYAL SOCIETY REPORT. Success of test, trace and isolate programmes depends on speed, compliance and monitoring, 27 May 2020. Acessado em 02 de fevereiro de 2021, disponível em https://royalsociety.org/news/2020/05/success-of-test-trace-and-isolate-programmes-depends-on-speed-compliance-and-monitoring/.

SARLET, Ingo W. Fundamentos Constitucionais: o Direito fundamental à proteção de dados, in Tratado de Proteção de Dados Pessoais, coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

SARLET, Ingo Wolfgang e KEINERT, Tania Margarete Mezzomo. O Direito Fundamental à Privacidade e as Informações em Saúde: Alguns Desafios, p. 121, in: ed. Keinert,Tania Margarete Mezzomo e others, in *Temas em Saúde*. São Paulo: Instituto de Saúde, 2015.

SHARMA, Omna; SULTAN, Ali A.; DING, Hong; TRIGGLE, Chris R.. A review of the progress and challenges od developing a Vaccine for COVID-19. Front Immunol. 2020; 11: 585354.Published online 2020 Oct 14. doi: 10.3389/fimmu.2020.585354. Acessaldo em 01 de fevereiro de 2021, disponível em https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7591699/

STRÖMHOLM. *Right of privacy and rights of the personality:* a comparative survey. Stockholm: Norstedt & Söners Förlag, 1967.

SUPREMO TRIBUNAL FEDERAL DO BRASIL, em decisão monocrática, divulgada em 27 de abril de 2020, a Ministra Rosa Weber, em resposta Medida Provisória (MPV) 954/2020, hoje revogada. Acessado em 15 de setembro de 2020, disponível em http://portal.stf.jus.br/processos/downloadPeca.asp?id=15342959354&ext=.pdf

THE BRITISH MEDICAL JOURNAL (Thebmj). Editorials Lessons in contact tracing from Germany, BMJ 2020;369:m2522. doi: https://doi.org/10.1136/bmj.m2522 (Published 25 June 2020). Acessado em 02 de fevereiro de 2021, disponível em https://www.bmj.com/content/369/bmj.m2522

THE LANCET DIGITAL HEALTH. Editorial: Contact tracing: digital health on the frontline; Volume. 2, Issue 11, E561, November 01, 2020. DOI: https://doi.org/10.1016/S2589-7500(20)30251-X. Acessado em 01 de fevereiro de 2021 e disponível em https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30251-X/fulltext

UNIÃO EUROPEIA E CONSELHO. EUR-Lex Regulamento Geral de Proteção de Dados (RGPD) Europeu e do Conselho, 2016/679, de 27 de abril de 2016, acessível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT – UNCTAD. Data Protection and Privacy legislation Worldwide. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Acessado em 13 de junho de 2020.

WOODHAMS, Samuel. COVID-19 Digital Rights Tracker. TOP10VPM. Acessível em https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/

UNIVERSIDADE DE MEDICINA JOHN HOPKINS - CORONAVIRUS RESOURCE CENTER, 2020. https://coronavirus.jhu.edu/map.html)

Preservação de Informações na Área da Saúde: aspectos morais, jurídicos e éticos à luz da Bioética

José Roberto Goldim[147]

RESUMO

A preservação de informações compreende aspectos morais, jurídicos e éticos. Os próprios conceitos de sigilo, segredo, confidencialidade, pudor e privacidade podem gerar confusões e ambiguidade entre os profissionais de saúde, A delimitação destes conceitos e a sua utilização na prática profissional é uma reflexão fundamental. Os desafios da ampliação do número de profissionais de saúde envolvido no atendimento dos pacientes, das suas relações com outras pessoas geram a necessidade de que estes termos sejam adequadamente esclarecidos.

PALAVRAS-CHAVE

Privacidade; Confidencialidade; Sigilo; Ética; Bioética.

[147] Biólogo, Doutor em Medicina. Chefe do Serviço de Bioética/Hospital de Clínicas de Porto Alegre/Brasil; Professor Adjunto da Escola de Medicina/Pontifícia Universidade Católica do Rio Grande do Sul; Professor Convidado da Faculdade de Medicina da Universidade Federal do Rio Grande do Sul.

Protecting Health Information: moral, legal and ethical aspects in a bioethical perspective

ABSTRACT

The preservation of information comprises moral, legal and ethical aspects. The very concepts of secrecy, confidentiality, and physical and informational privacy can generate confusion and ambiguity among health professionals. The delimitation of these concepts and their use in professional practice is a fundamental reflection that must be carried out. The challenges of expanding the number of health professionals involved in patient care, in their relationships with other people, generate the necessity that these terms be adequately clarified.

KEYWORDS

Privacy, Confidentiality, Secrecy, Ethics, Bioethics.

1. Alguns aspectos históricos

A preservação de informações é um tema que acompanha a área da saúde desde os seus primórdios. Estas manifestações se deram, especialmente, no âmbito da Moral Médica e de Ética Médica. A primeira estabelecendo regras de conduta aos médicos e a segunda dando justificativas de por que este comportamento é adequado (Vasques, 2000).

A Escola de Medicina da Ilha de Cós, fundada por Hipócrates, no século 5 aC, tinha um ritual de iniciação onde todos os alunos faziam um juramento no início de seus estudos. Este juramento estabelecia um comprometimento moral, assumido perante várias divindades então associadas à Saúde e à Medicina, incluía a proteção às informações recebidas pelo médico. No texto do Juramento Hipocrático havia a seguinte obrigação:

> "qualquer coisa que eu veja ou ouça, profissional ou privadamente, que não deve ser divulgada, eu conservarei em segredo e a ninguém contarei" (Hippocrates, 1923).

É interessante notar que, desde o início, o dever de preservação das informações recebidas ou percebidas pelo médico tinham a possibilidade de serem compartilhadas, em caráter de exceção. No juramento hipocrático a preservação incluía todas as informações de pacientes, às quais o médico teve acesso, e não apenas as obtidas no exercício profissional.

Na Índia, ao redor do ano 100dC, um documento denominado de Charaka Samhita, continha um Juramento de Iniciação do Médico. Neste juramento também havia a clara indicação de "cumprir escrupulosamente o sigilo médico" (Veatch, 1997).

Na primeira conferência dada por John Gregory, na Faculdade de Medicina de Edinburgo, sobre os deveres e qualificações do médico, no ano de 1772, ele faz um comentário sobre a questão do acesso do médico às informações sobre a vida privada dos seus pacientes e o dever moral de proteção associado.

> "Um médico, pela natureza de sua profissão, tem muitas oportunidades de conhecer o caráter privado e as preocupações das famílias com as quais trabalha. Além do que pode aprender pela sua própria observação, muitas vezes é admitido na confiança daqueles que talvez se sintam obrigados a entregarem a sua vida aos seus cuidados. Ele vê as pessoas nas circunstâncias mais degradantes, muito diferentes daquelas em que o mundo as vê; oprimidas pela dor, enjoo e desânimo. Nessas situações humilhantes, em vez da costumeira alegria, temperamento equilibrado e vigor mental, ele encontra rabugice, impaciência e acanhamento. Portanto, parece que o caráter dos indivíduos, e a confiança das famílias, pode às vezes depender da discrição, do sigilo e da honra de um médico. O sigilo é particularmente necessário no que diz respeito às mulheres" (Gregory, 1772).

Na mesma Escola de Medicina de Edinburgo, Thomas Percival, que foi aluno de John Gregory, escreveu o livro que funda a Ética Médica – Medical Ethics, em 1803. Este livro, com o subtítulo: Código de Institutos e Preceitos Adaptados à Conduta Profissional de Médicos e Cirurgiões. O texto é uma coletânea de casos e situações vivenciadas por Thomas Percival ao longo de sua carreira. Na dedicatória do livro para seu segundo filho, que estava se formando em Medicina, utilizou a denominação de "pequeno Manual de Ética Médica". Neste mesmo texto introdutório, ele propôs que a Ética Profissional deve:

> "revigorar e ampliar a sua compreensão; enquanto o cumprimento dos deveres que devem ser apreciados, suavizarão os seus modos, ampliarão os seus afetos, e o formarão para aquela conduta digna e adequada, essencial ao caráter de um cavalheiro"(Percival, 1987).

Neste texto não são apresentadas apenas regras de conduta, como prescrições, mas sim como fundamentação, como uma justificativa associada às ações prescrita. É nesta proposta que é abordada a questão da preservação das informações:

> "Nas grandes enfermarias de um hospital, os pacientes devem ser questionados quanto às suas queixas, em tom de voz que não possa ser ouvido por acaso. O sigilo, também, quando exigido por circunstâncias peculiares, deve ser rigorosamente observado. E as mulheres sempre devem ser tratadas com a mais escrupulosa delicadeza. Negligenciar ou brincar com seus sentimentos é crueldade; e toda ferida, assim infligida, tende a produzir uma mente insensível, um desprezo pelo decoro e uma insensibilidade ao pudor e à virtude. Essas considerações devem ser insistentemente incentivadas com os alunos do hospital" (Percival, 1987).

As ideias propostas por Thomas Percival rapidamente se disseminaram. A Associação Médica Americana (AMA), em 1847 propôs o primeiro Código de Ética Médica, utilizando este referencial ético. Escreveram um documento que mescla aspectos morais e éticos da conduta médica considerada como sendo adequada. A rigor, este documento fez uma codificação da Ética Médica. A questão da preservação de informações foi incluída logo na abertura do documento, no segundo parágrafo do primeiro artigo do Código:

> "Capítulo 1 – Dos deveres dos médicos para com seus pacientes e as obrigações dos pacientes para com seus médicos
> Art. 1 – Deveres dos médicos para os seus pacientes
> Sigilo e delicadeza, quando exigidos por circunstâncias peculiares, devem ser estritamente observados; e as relações familiares e confidenciais, que são reveladas aos médicos em suas visitas profissionais, devem ser usadas com discrição e com o mais escrupuloso respeito à fidelidade e honra. A obrigação de sigilo se estende além do período de serviços profissionais; nenhum dos segredos da vida pessoal e doméstica, nenhuma enfermidade de disposição ou defeito de caráter observada durante o atendimento profissional, jamais deverão ser divulgados por ele, exceto quando for imperativamente exigido a fazê-lo. A força e a necessidade desta obrigação são de fato tão grandes, que os profissionais foram, sob certas circunstâncias, protegidos por tribunais

de justiça, em sua observância do segredo" (American Medical Association - AMA, 1847).

2. Os aspectos morais e os códigos profissionais

Este primeiro Código de Ética Médica, estabelecido pela AMA, serviu de base para a elaboração de inúmeros outros documentos semelhantes em vários países do mundo, como o Brasil e Portugal.

No atual Código de Ética Médica do Brasil, proposto pelo Conselho Federal de Medicina, em 2018, a proteção às informações e a exposição do paciente constam em três diferentes partes do documento: no Capítulo I - Princípios Fundamentais; no capítulo IV – Direitos Humanos; e no Capítulo IX – Sigilo Profissional. Em seus diversos artigos, são explicitadas algumas situações que permitem caracterizar melhor a questão da proteção das informações e da exposição do paciente. Algumas situações especiais, como as envolvendo pacientes menores de idade (Art. 74); a identificação de pacientes em divulgação leiga e científica (Art. 75); atendimento de trabalhadores (Art. 76); prestar informações às seguradoras (Art. 77); a orientação de auxiliares e alunos (Art. 78); e nas questões envolvendo cobrança de honorários profissionais (Art. 79) (Conselho Federal de Medicina - CFM, 2018). Vale destacar o texto de alguns destes artigos:

> "Capítulo I - Princípios Fundamentais
> XI - O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei.
>
> Capítulo IV – Direitos Humanos
> É vedado ao médico:
> Art. 38. Desrespeitar o pudor de qualquer pessoa sob seus cuidados profissionais.
>
> Capítulo IX – Sigilo Profissional
> É vedado ao médico:
> Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.
> Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha (nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento); c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal." (Conselho Federal de Medicina - CFM, 2018).

A Ordem dos Médicos de Portugal, em 2016, por meio do Regulamento 707/2016, estabeleceu o Regulamento de Deontologia Médica. Este documento assume uma denominação correta, pois apresenta um conjunto de normas deontológicas que os médicos devem seguir no exercício da sua profissão. Este documento dedica todo o

Capítulo IV às questões envolvendo o Segredo Médico. São dez artigos que abordam múltiplas questões desde o conceito do que é segredo médico (Art. 29), em que âmbito ele é mandatório (Art. 30); as suas aplicações em diversas áreas de atuação profissional (Art. 31); as situações que podem excluir o cumprimento deste dever (Art. 32); as precauções associadas (Art. 33); a manutenção deste dever mesmo em situações de cobrança de honorários (Art. 34); dos dados informatizados (Art. 35); do tratamento das informação da saúde (Art. 37); e da responsabilidade do médico em funções diretivas (Art. 38). Além destes, o Capítulo V - Informação médica e Processo clínico, em seu Art. 42, sobre publicações cientificas, veda a identificação dos doentes, salvo quando tiver uma autorização expressa para tal (Ordem dos Médicos de Portugal, 2016). Dois destaques são importantes:

> "Artigo 29.º O segredo médico
> O segredo médico é condição essencial ao relacionamento médico-doente, assenta no interesse moral, social, profissional e ético, que pressupõe e permite uma base de verdade e de mútua confiança.
>
> Artigo 30.º Âmbito do segredo médico
> 1 — O segredo médico impõe -se em todas as circunstâncias dado que resulta de um direito inalienável de todos os doentes.
> 2 — O segredo abrange todos os factos que tenham chegado ao conhecimento do médico no exercício da sua profissão ou por causa dela e compreende especialmente: a) Os factos revelados diretamente pela pessoa, por outrem a seu pedido ou por terceiro com quem tenha contactado durante a prestação de cuidados ou por causa dela;
> b) Os factos apercebidos pelo médico, provenientes ou não da observação clínica do doente ou de terceiros;
> c) Os factos resultantes do conhecimento dos meios complementares de diagnóstico e terapêutica referentes ao doente;
> d) Os factos comunicados por outro médico ou profissional de saúde, obrigado, quanto aos mesmos, a segredo.
> 3 — A obrigação de segredo médico existe, quer o serviço solicitado tenha ou não sido prestado e quer seja ou não remunerado.
> 4 — O segredo médico mantém-se após a morte do doente.
> 5 — É expressamente proibido ao médico enviar doentes para fins de diagnóstico ou terapêutica a qualquer entidade não vinculada ao segredo médico" (Ordem dos Médicos de Portugal, 2016).

3. Os aspectos jurídicos

A preservação das informações na área da saúde, além dos aspectos éticos e morais, também tem uma longa tradição jurídica. Tanto o Direito, assim como a Moral, têm esta característica prescritiva (Habermas, 2004), pois buscam estabelecer uma previsibilidade para as ações humanas, com a finalidade de buscar organizar a vida em comunidade. São

perspectivas complementares a da Ética, que visa buscar justificativas de adequação para estas mesmas ações (Vasques, 2000).

Inúmeras legislações contemplam estas questões, como o Regulamento Geral de Proteção de Dados da Europa (Parlamento Europeu, 2016) e a Lei Geral de Proteção de Dados do Brasil (Brasil, 2018). No Brasil, a preservação das informações obtidas por profissionais da saúde, também já estavam estabelecidas no Código Penal (Brasil, 1940) e no Código Civil (Brasil, 2002).

Alguns casos judiciais também serviram para elucidar conceitos e entendimentos a respeito do que seja sigilo profissional, confidencialidade e privacidade. O caso Tarasoff ("Tarasoff vs. Regents of the University of California. California Supreme Court," 1976), ocorrido na década de 1970, é um caso paradigmático nesta área. Este caso, envolvendo um assassinato premeditado e discutido previamente pelo autor, na condição de paciente, com profissionais de saúde. Este caso gerou uma ampla reflexão dos limites do sigilo profissional.

No julgamento foram discutidas duas diferentes perspectivas a respeito do sigilo profissional: da confidencialidade dos profissionais e da privacidade do paciente. O voto do relator foi pela revelação da situação de risco. Ele baseou a sua argumentação no critério de que a defesa da vida é um dever prioritário, que ultrapassa ao da confidencialidade ("Tarasoff vs. Regents of the University of California. California Supreme Court," 1976). O juiz entendeu que a confidencialidade era um dever *prima facie*, ou seja, que poderia ser descumprido quando, em uma situação particular, houvesse outro dever conflitante de maior relevância (Ross, 1930).

O voto dissidente, ao contrário, foi pela preservação das informações compartilhadas no ambiente de saúde. A argumentação foi no sentido de que a confidencialidade é um direito inalienável do paciente. Este caso serviu de paradigma para este tipo de situação, quando existe um terceiro em risco. Neste caso se justifica a quebra de confidencialidade eticamente justificada ("Tarasoff vs. Regents of the University of California. California Supreme Court," 1976).

4. A perspectiva da Bioética

O surgimento da Bioética permitiu consolidar inúmeros aspectos relacionados a este tema. A Bioética se utiliza de várias fontes para realizar as suas reflexões. Na Bioética contemporânea os inúmeros referenciais éticos, as perspectivas morais e os aspectos

jurídicos são utilizados em uma perspectiva interdisciplinar, compartilhada e complexa (Goldim, 2006).

Existem confusões e ambiguidades associadas ao uso dos conceitos de segredo, sigilo, privacidade e confidencialidade. As fronteiras entre estes conceitos, para muitas pessoas, não ficam muto clara, ficam como que com suas "bordas borradas" (Wittgenstein, 1999).

Segredo, segundo a sua definição, é "aquilo que a ninguém deve ser revelado, que é secreto, sigiloso" (Houaiss, Villar, & Franco, 2001). Por sua vez, sigilo é definido como "aquilo que permanece escondido da vista ou do conhecimento, segredo", ou ainda, "coisa ou notícia que não se pode revelar ou divulgar, segredo" (Houaiss et al., 2001). Ambos, segredo e sigilo, remetem um ao outro, sempre na perspectiva do impedimento da divulgação.

A confidencialidade está radicalmente associada a prática humana de compartilhar e preservar segredos (Bok, 1984). O compartilhamento de segredos permite estabelecer ou manter um relacionamento mais íntimo com outras pessoas. A confidencialidade envolve a comunicação de informações pessoais e privadas de uma pessoa a outra, na presunção de que estas mesmas informações não serão reveladas a outras pessoas. Ou seja, outras pessoas somente poderão ter acesso a estas informações quando houver uma autorização expressa e específica (Winslade, 2005). A confidencialidade tem dois âmbitos essenciais: facilitar uma comunicação sensível e excluir pessoas não autorizadas ao acesso a estas informações (Winslade, 1978).

Os Códigos de Ética ou de Deontologia Profissional seguem utilizando as expressões sigilo (Conselho Federal de Medicina - CFM, 2018) ou segredo profissional (Ordem dos Médicos de Portugal, 2016). Estas denominações poderiam ser consideradas adequadas quando a relação profissional-paciente era entre duas pessoas. Na prática atualmente vigente na área da saúde, o atendimento é multiprofissional, ou seja, inúmeros profissionais atuam colaborativamente com o mesmo paciente. Todos os profissionais registram suas informações em um prontuário do paciente, que é de uso comum a todos. Nesta nova conformação profissional, melhor que utilizar os conceitos de sigilo ou segredo, é denominar o dever de proteger as informações do paciente como sendo confidencialidade. No atendimento realizado por vários profissionais, é possível manter a confidencialidade e compartilhar as informações de forma adequada, desde que autorizadas pelo paciente e no seu melhor interesse (Francisconi & Goldim, 1998). É fundamental manter esta perspectiva do "acesso às informações no melhor interesse do

paciente" quando outras pessoas e instituições estão envolvidas, novamente as "bordas borradas" podem voltar a estar presentes, agora em relação aos limites de adequação.

A confidencialidade, entendida como um dever *prima facie*, permite que em situações muito especiais e adequadamente justificadas, estas informações possam ser compartilhadas, com a finalidade de proteger o próprio paciente ou a terceiros envolvidos. A partir do caso Tarasoff, foram estabelecidos critérios para a avaliação destes conflitos entre deveres. A quebra de confidencialidade somente é eticamente admitida quando: a) um sério dano físico, a uma pessoa identificável e específica, tiver alta probabilidade de ocorrência; b) um benefício real resultar desta quebra de confidencialidade; c) for o último recurso, após ter sido utilizada persuasão ou outras abordagens, e, por último, d) este procedimento deve ser generalizável, sendo novamente utilizado em outra situação com as mesmas características, independentemente de quem seja a pessoa envolvida (Junkerman, C; Schiedermayer, 1998). Em outras situações, previstas em lei, é possível o compartilhamento de informações entre pessoas ou instituições, desde que haja o compromisso de confidencialidade entre os envolvidos, como no caso da comunicação de doenças transmissíveis para a autoridade sanitária.

A privacidade pode ser entendida como sendo a limitação do acesso às informações de uma dada pessoa, ao acesso à própria pessoa, à sua intimidade, envolvendo as questões de anonimato, sigilo, afastamento ou solidão. É a liberdade que o paciente tem de não ser observado sem autorização (*Kennedy Institute of Ethics. Bioethics Thesaurus. [privacy]*, 1995). É possível estabelecer, desta forma, dois âmbitos complementares para privacidade: a privacidade física, ou corpora, e a informacional (Allen, 2003).

A privacidade física se refere ao acesso ao corpo, a observação direta ao paciente. Pode ser entendida como o respeito ao pudor, já previsto em alguns documentos deontológicos (Conselho Federal de Medicina - CFM, 2018). É muito importante associar este acesso ao corpo do paciente, seja pelo toque ou pela sua visibilidade, às questões de privacidade corporal. Muitas vezes os profissionais de saúde banalizam o toque no corpo do paciente, que pode se sentir invadido em seu espaço corporal. Da mesma forma, nas instituições de saúde existe a circulação de muitas e diferentes pessoas, atendendo em regime de plantão; são inúmeros sistemas de segurança por meio de câmeras de vídeo; o próprio uso de vídeo chamadas ou obtenção de fotos e filmagens pelos pacientes ou seus familiares, são situações de risco à preservação da privacidade corporal dos pacientes, dos profissionais de saúde, dos familiares ou de outras pessoas que circulam nestes

ambientes. Na medida em que os cuidados se intensificam, a exposição corporal aumenta. Em um depoimento pessoal, uma paciente afirmou: “quando se está internado em uma unidade de tratamento intensivo, o pudor fica lá fora”.

A privacidade informacional, por outro lado, se refere aos registros, aos dados do paciente que os profissionais simplesmente tiveram acesso e aqueles que estão documentados no prontuário, em registros de exames ou em imagens que ficam armazenadas (Allen, 2003). Este tem sido o foco principal de preocupação nas instituições de saúde: estabelecer sistemas seguros para este conjunto gigantesco de informação. Os sistemas podem ser seguros, mas o uso das informações ali contidas pode não ser. Inúmeras situações de vazamentos de dados, adequadamente protegidos na instituição, ocorreram por falta de cuidado dos profissionais ou outras pessoas que tiveram acesso a estas informações. Sem contar os acessos intencionais com esta finalidade.

A metáfora utilizada, para caracterizar o espaço privado e o espaço público, do jardim e da praça é muito útil (Saldanha, 1986). Os espaços onde os cuidados de saúde ocorrem não são “praças”, mas sim “jardins ampliados”. Podem ter uma área mais ampla, compartilhada com outras pessoas, mas continuam com a mesma necessidade de proteção deste direito das pessoas.

A noção de privacidade, como um direito fundamental das pessoas, também pode ser alterada na perspectiva da saúde. A perspectiva da própria saúde se alterou do plano individual para um plano mais ampliado, em função do risco para terceiros. Isto pode ser aplicado, por exemplo, em situações de doenças familiares, de aconselhamento genético ou reprodutivo (Stoll de Morais, Ashton-Prolla, Goldim, & Santana Fernandes, 2018). Isto não deve ser entendido como uma perda da noção de privacidade, mas sim uma ampliação do seu conceito para além do plano pessoal. Tem informações de saúde que podem e devem ser compartilhadas em um âmbito maior, mas igualmente restrito. A privacidade relacional permite compartilhar informações que podem beneficiar os membros de uma família a partir de um diagnóstico de uma doença com repercussão para outras pessoas. Esta possibilidade tem que ser compartilhada com o paciente, ou com a pessoa que solicitou um aconselhamento, previamente a geração das informações. Esta pessoa não pode ser surpreendida, mas sim adequadamente informada das diferentes possibilidade de ampliação do compartilhamento destas informações (Goldim & Gibbon, 2015).

Em algumas culturas, a noção de privacidade individual não é usual. A perspectiva de privacidade individual das culturas europeia e norte-americana contrasta com a privacidade comunitária de culturas africanas. O conceito de Ubuntu, de que o indivíduo só existe em sociedade, gera esta perspectiva (Ndebele, Mfutso-Bengo, & Masiye, 2008). É interessante verificar, contudo, a aproximação possível de ser realizada com esta perspectiva e o referencial da Alteridade, onde a presença do outro é que me legitima, a presença do outro é que me dá identidade, gerando uma relação, uma copresença ética e uma corresponsabilidade (Lévinas, 1997).

6. Considerações finais

A preservação das informações deve ser entendida por todos como uma necessidade. Uma necessidade compreendida, quando reconhecida como um direito à privacidade, e uma necessidade objetivada, quando gera deveres de confidencialidade.

O princípio da precaução é um elemento fundamental nesta reflexão, pois reconhece que a existência de um risco de dano sério e irreversível requer a implementação de ações que possam prevenir ou minimizar a sua ocorrência. O adequado entendimento das relações entre os aspectos morais, jurídicos e éticos, em uma perspectiva integradora, é fundamental. Este é o nosso desafio.

7. Referências bibliográficas

Allen, A. (2003). Privacy. In S. G. Post (Ed.), *Enciclopedia of Bioethics* (3rd ed., pp. 2120–2130). Detroid: Gale.

American Medical Association - AMA. (1847). *Code of Medical Ethics*. Chicago: AMA.

Bok, S. (1984). *Secrets: on the Ethics od Concealment and Revelation.* New York: Oxford University Press.

Brasil. (1940). *Código Penal. Decreto-lei 2848/40*. Retrieved from http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

Brasil. (2002). *Código Civil. Lei 10.406/2002*. Retrieved from http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm

Brasil. (2018). *Lei Geral de Proteção de Dados Lei 13709/2018*. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm

Conselho Federal de Medicina - CFM. (2018). *Código de Ética Médica (Resolução CFM n° 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019)*. Brasília: CFM. Retrieved from http://www.cremesp.org.br/library/modulos/publicacoes/pdf/CodigoEticaMedica20

13.pdf

Francisconi, C. F. M., & Goldim, J. R. (1998). Aspectos Bioéticos da Confidencialidade e da Privacidade. In S. I. F. Costa, V. Garrafa, & G. W. Oselka (Eds.), *Iniciação a Bioética* (pp. 269–284). Brasilia: CFM.

Goldim, J. R. (2006). Bioética: Origens e Complexidade. *Revista HCPA*, *26*(2), 86–92. Retrieved from https://www.ufrgs.br/bioetica/complex.pdf

Goldim, J. R., & Gibbon, S. (2015). Between personal and relational privacy: understanding the work of informed consent in cancer genetics in Brazil. *Journal of Community Genetics*, *6*, 287–293. https://doi.org/10.1007/s12687-015-0234-4

Gregory, J. (1772). *Lectures on the duties and qualifications of a physician*. London: W. Strahan and T. Cadell. Retrieved from https://books.google.com.br/books/about/Lectures_on_the_Duties_and_Qualification.html?id=iKpUwIKMv40C&redir_esc=y

Habermas, J. (2004). *O futuro da natureza humana: a caminho de uma eugenia liberal?* (1st ed.). São Paulo: Martins Fontes.

Hippocrates. (1923). *Vol. I - Ancient Medicine. Airs, Waters, Places. Epidemics 1 and 3. The Oath. Precepts. Nutriment*. Boston: Harvard University Press.

Houaiss, A., Villar, M. de S., & Franco, F. M. de M. (2001). *Dicionário Houaiss da língua portuguesa* (1st ed.). Rio de Janeiro: Objetiva.

Junkerman, C; Schiedermayer, D. L. (1998). *Practical Ethics for Students, Interns, and Residents: A Short Reference Manual* (2nd ed.). Frederick, Md.: University Publishing Group.

Kennedy Institute of Ethics. Bioethics Thesaurus. [privacy]. (1995). Washington (DC): KIE. Retrieved from http://www.bioetica.ufrgs.br/privacid.htm

Lévinas, E. (1997). *Entre nós: Ensaios sobre a alteriedade*. (P. S. Pivitto, E. A. Kuiava, J. Nedel, L. P. Wagner, & M. L. Pelizolli, Eds.) (Vozes). Petrópolis.

Ndebele, P., Mfutso-Bengo, J., & Masiye, F. (2008). HIV/AIDS reduces the relevance of the principle of individual medical confidentiality among the Bantu people of Southern Africa. *Theoretical Medicine and Bioethics*, *29*(5), 331–340. https://doi.org/10.1007/s11017-008-9084-y

Ordem dos Médicos de Portugal. (2016). *Regulamento n.o 707/2016 - Regulamento de Deontologia Médica. Diário da República, 2.a série — N.o 139 — 21 de julho de 2016:22576-22588.* Retrieved from http://ordemdosmedicos.pt/wp-content/uploads/2017/08/Regulamento_707_2016__Regulamento_Deontológico.pdf

Parlamento Europeu. (2016). *Regulamento (UE) 2016/679*. *Jornal Oficial da União Europeia* (Vol. 2014). Retrieved from

https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf

Percival, T. (1987). *Medical Ethics*. Manchester: S. Russell.

Ross, W. D. (1930). *The right and the good*. Oxford: Clarendon.

Saldanha, N. (1986). O jardim e a praça: Ensaio sobre o lado privado e o lado público da vida social e histórica. *Ci. & Tróp, Recife*, *3*(091), 48. Retrieved from https://periodicos.fundaj.gov.br/CIC/article/view/326

Stoll de Morais, L., Ashton-Prolla, P., Goldim, J. R., & Santana Fernandes, M. (2018). Privacidade relacional no Ambulatório de Oncogénetica do Hospital de Clínicas de Porto Alegre. *Revista Brasileira de Políticas Públicas*, *8*(3), 1689–1699. https://doi.org/10.5102/rbpp.v8i3.5638

Tarasoff vs. Regents of the University of California. California Supreme Court. (1976), (17 California Reports, 3rd series, 425. Decided July, 1, 1976). Retrieved from https://law.justia.com/cases/california/supreme-court/3d/17/425.html

Vasques, A. S. (2000). *Ética*. Rio de Janeiro: Civilização Brasileira.

Veatch, R. M. (1997). *Medical Ethics* (2nd ed.). Sudbury: Jones and Bartlett.

Winslade, W. J. (1978). Confidentiality. In W. T. Reich (Ed.), *Enciclopedia of Bioethics* (pp. 194–200). New York: The Free Press.

Winslade, W. J. (2005). Confidentiality. In S. G. Post (Ed.), *Enciclopedia of Bioethics* (3rd ed.). Detroid: Gale.

Wittgenstein, L. (1999). *Investigações filosóficas*. São Paulo: Nova Cultural.

A Inteligência Artificial e o Ecossistema Industrial na sua relação com as Patentes na Área da Saúde: uma abordagem jurídica e antropocêntrica sobre os desafios impostos em tempos de pandemia

Cristina Maria de Gouveia Caldeira[148]
Gabrielle Bezerra Sales Sarlet[149]

RESUMO

Mediante uma investigação bibliográfica, exploratória e utilizando o método hipotético-dedutivo, são analisados os desafios à proteção de dados pessoais suscitados pela aplicação da inteligência artificial e do *big data* em tempos de Covid-19. Reflete-se sobre o equilíbrio necessário entre custos e benefícios da atribuição de patentes e a garantia do acesso a medicamentos inovadores, em especial no contexto europeu, bem como a inovação e a sustentabilidade da indústria farmacêutica europeia. Analisa-se a implementação da inteligência artificial em conformidade com a política de proteção dos dados relativos à saúde e aos dados genéticos, à luz dos instrumentos jurídicos de direito europeu. Acompanhamos os esforços desenvolvidos pela União Europeia e pelas suas instituições, para assegurar a proteção dos direitos humanos fundamentais face às novas tecnologias, ao mesmo tempo que os cientistas, maximizando o volume de dados atualmente gerado e o uso da inteligência artificial, apresentam ao mundo uma inovação terapêutica sem precedentes. Parte-se dos pilares éticos da inteligência artificial rumo a uma proposta de enquadramento legal, baseada na confiança e no risco. Por fim, torna-se obrigatória uma reflexão mais adensada sobre a ética na ciência, as tecnologias computacionais inteligentes e a saúde, na sua relação com o direito de propriedade intelectual e os direitos humanos e fundamentais, num ecossistema industrial de contornos jurídicos e civilizacionais.

PALAVRAS-CHAVE

inteligência artificial, informação de saúde, direitos humanos e fundamentais, direitos industriais, patentes.

---

[148] Pós-Doutorada na área da Propriedade Intelectual, Universidade Nova de Lisboa e investigadora de pós-doutoramento na Pontifícia Universidade Católica (PUCRS), Brasil. 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. Colabora no Laboratório de Bioética no Hospital de Clínicas (RS Brasil), como investigadora na área de proteção de Tecnologia e Ensino Superior. Coautora de projetos de diplomas legais. Foi Vice-Reitora do IADE-U – Instituto de Arte, Design e Empresa – Universitário (2014-2015). É Diretora Executiva e Editorial da Revista *Privacy and Data Protection Magazine* e Cocoordenadora *Privacy and Data Protection Centre.* Autora de várias publicações e participante regular em iniciativas públicas de Direito da Propriedade Intelectual e Proteção de Dados. *Curriculum vitae:* Ciência ID: 711B-87B9-6826. ORCID ID: https://orcid.org/0000-0001-6925-1877.

[149] Pós-doutora em Direito pela Universidade de Hamburgo-Alemanha. Pós-doutora em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Doutora em Direito pela Universidade de Augsburg - Alemanha. Mestre e graduada em Direito pela Universidade Federal do Ceará (UFC). Ex-bolsista do MPI - Max Planck Institute Hamburg-Alemanha. Professora do curso de graduação e de pós-graduação em Direito na Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Especialista em Neurociências e comportamento na PUC-RS. Atualmente, encontra-se em formação em psicanálise freudiana no Circulo Freudiano de Psicanalise do Rio Grande do Sul. E-mail: gabriellebezerrasales@gmail.com. Currículo: http://lattes.cnpq.br/9638814642817946. ORCID ID - https://orcid.org/0000-0003-3628-0852

Artificial Intelligence and the Industrial Ecosystem in the face of Health Patents: a legal and anthropocentric approach to the challenges imposed by pandemic times

ABSTRACT

Through bibliographical, exploratory research and using the hypothetical-deductive method, the challenges to the protection of personal data raised with the use of artificial intelligence and big data in Covid-19 times are analyzed. This article reflects on the necessary balance between costs and benefits of patent births and, at the same time, the guarantee of access to innovative medicines, especially in the European context, as well as on the innovation and sustainability of the European pharmaceutical industry. The implementation of artificial intelligence is analyzed in accordance with the policy for the protection of health-related data and genetic data, in line with the legal instruments of European law. We follow the efforts made by the European Union and its institutions to ensure the protection of human rights in the face of new technologies, while scientists maximize the volume of data currently generated and the use of AI for special innovation. It starts from the ethical pillars of artificial intelligence to the hypothesis of a legal framework based on the equation of trust and risk. Finally, it becomes mandatory to reflect more deeply on ethics in science, intelligent computational technologies and health in its relationship with intellectual property rights and human fundamental rights, in an industrial ecosystem with legal and civilizational boundaries.

KEYWORDS

artificial intelligence, health information, human and fundamental rights, industrial rights, patents.

Introdução

Definida como *"*um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional*"*[150], a inteligência artificial (IA) é exibida por meio de máquinas que mimetizam "certas funções cognitivas que são caraterísticas da mente humana"[151], distinguindo-se em forte e fraca dependendo da sua complexidade.

Aplica-se em sistemas que apresentam um comportamento inteligente, capazes de analisar o ambiente e atuar com um determinado nível de autonomia, de modo a atingir objetivos específicos, cobrindo várias áreas, desde os motores de busca, os assistentes pessoais, veículos automatizados, robôs humanoides e sociais até às armas autónomas. Este crescimento tão acentuado é indissociável dos avanços em *data science*, baseando-se cada vez mais em métodos de aprendizagem automática, treinados com recurso a uma grande quantidade de dados.

Um dos fatores que contribuíram para o seu crescimento foi o desenvolvimento de métodos de treino de redes neuronais profundas que promovem o reconhecimento da fala, da imagem, bem como da capacidade de detetar, de modelar ou de exibir comportamentos afetivos como emoções, humor, atitudes e personalidades, dando os primeiros passos na direção da inteligência artificial emocional, ou seja, de sistemas inteligentes dotados de capacidade social e eventualmente de moralidade.

A Inteligência Artificial entrou numa nova era, transformando-se numa das áreas de investigação científica multidisciplinar mais complexas[152], mas igualmente promissora. De facto, a dificuldade em prever o comportamento de produtos dotados de IA, bem como de compreender as possíveis causas de danos, levou a Comissão Europeia e a Presidência portuguesa do Conselho da União Europeia[153], a se concentrarem na elaboração de um primeiro quadro regulamentar da IA. Nessa matéria, é grande a expetativa depositada no debate informal agendado para o dia 23 de abril de 2021, entre a Diretora da IA e Lucilla Sioli, da Indústria digital da DG CONNECT da Comissão Europeia, onde será apresentada "*A European approach to the regulation of artificial intelligence*", a que seguirá uma ronda de primeiras impressões sobre o conteúdo da proposta.

---

[150] COM(2020) 65, p. 2.
[151] VICENTE, Dário Moura, «Inteligência Artificial e Iniciativas Internacionais», 2020, p.93-105.
[152]PARLAMENTO EUROPEU. Relatório sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial, 2.10.2020.
[153] Portugal preside ao Conselho da União Europeia durante o primeiro semestre de 2021.

A criação de uma iniciativa legislativa para enquadrar a IA já se encontrava mencionada no «Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica», apresentado pela Comissão Europeia, no dia 19 de fevereiro de 2020. Nesse Relatório, é referido que as grandes quantidades de dados envolvidos, a dependência de algoritmos e a opacidade do processo decisório dos sistemas de inteligência artificial tornam mais difícil prever o comportamento de produtos com inteligência artificial e compreender as possíveis causas de danos[154].

É consensual que a dependência de algoritmos e a opacidade do processo decisório dos sistemas de IA estão na base da decisão de criar uma estrutura regulatória abrangente para a inteligência artificial, em defesa da transparência e da tutela dos direitos fundamentais. Nessa conformidade, a proposta que se encontra em análise, integra aspetos essenciais designadamente, a definição de aplicações de alto risco, a regulação dos fornecedores de sistemas de IA, a vigilância pós-mercado de IA, a avaliação da conformidade das aplicações de IA de alto risco e a criação de um novo conselho consultivo placa a IA.

O eurodeputado alemão Axel Voss (PPE) defende "um quadro de responsabilidade civil orientado para o futuro, responsabilizando estritamente os operadores de IA de alto risco por quaisquer danos causados. Defende que um quadro jurídico claro estimularia a inovação, fornecendo uma base legal às empresas, ao mesmo tempo que protegeria os cidadãos e promoveria a confiança nas tecnologias IA[155].

Independentemente da abordagem jurídica da IA que vier a ser criada, deve ser complementada com uma visão antropocêntrica. A esse propósito, acompanhamos o pensamento de Antônio Anselmo Martino:

> "We are also forgetting one important thing: machines can do calculations at extraordinary speeds, read a lot of information and store it, but what they cannot do is to weigh. Weighing is typical of human beings and their culture and therefore will be weighted differently according to time and place, but it is about using values and being able to distinguish what is most important and least important, urgent and ordinary. Therefore, for now, we are confident that no machine will govern our lives beyond what we allow."[156]

---

[154] COM(2020) 64 final, p.2.

[155] PARLAMENTO EUROPEU. «Regular a Inteligência Artificial na UE: as propostas do Parlamento», 26.03.2021, p.3.
https://www.europarl.europa.eu/pdfs/news/expert/2020/10/story/20201015STO89417/20201015STO89417_pt.pdf

[156] MARTINO, A. Anselmo. «Logic, Informatics, Artificial Intelligence And Technology, 2020, p.46 e 47.

Importa, no entanto, salientar que a principal aplicação da IA ocorre por via da robótica, sobre a qual o Parlamento Europeu já apresentou uma Resolução, 2017, propondo à Comissão Europeia a adoção de mecanismos de responsabilidade objetiva dos robôs, complementado com a criação de um estatuto jurídico próprio e um sistema de seguros obrigatório para compensações, entre outras disposições[157], admitindo que,

> "a humanidade se encontra no limiar de uma era em que robôs, «bots», androides e outras manifestações de inteligência artificial (IA), cada vez mais sofisticadas, parecem estar preparados para desencadear uma nova revolução industrial, que provavelmente não deixará nenhuma camada da sociedade intacta, é extremamente importante que o legislador pondere as suas implicações e os seus efeitos a nível jurídico e ético, sem pôr entraves à inovação".

No mesmo sentido, Antônio Anselmo Martino reforça que:

> "Robotics is just a singular field of A.I., but we're afraid of a robot running our lives. The fears that accompany humanity created the Golem of Rabbi Levi, Frankenstein from an English writer, Mary Shelley. And other fantastic characters that scare us fear and love two sources of creation. Instead of dealing with current issues such as health, work, environmental balance, education, politics and human coexistence, there are human attacks on A.I. systems to pollute data and confuse the algorithms that are at the base of the intelligent systems developed by the European Sherpa project.[158]"

Independentemente das reservas acima suscitadas, importa realçar que a robótica é hoje indispensável a diversos setores da sociedade, tendo um especial impacto na área da saúde, designadamente, no tratamento de doenças crónicas, em diagnósticos radiológicos, na automatização da análise de amostras clínicas e radiografias ou exames bidimensionais, entre outros[159].

Na sequência da Resolução do Parlamento Europeu, a Comissão Europeia criou o *Plano Coordenado para a Inteligência Artificial*[160] bem como uma *Estratégia para a Inteligência Artificial*, iniciativas que encontram acolhimento no *Programa Horizonte*

---

[157] PARLAMENTO EUROPEU. Resolução que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica, de 16 de fevereiro de 2017.

[158] MARTINO, Antônio Anselmo. «Logic, Informatics, Artificial Intelligence and Technology in Law: History And Challenges» in *Law, Tecnologhy and Innovation*, 2020, p.45.

[159] A *machine learning*, técnica em que o computador "lê" previamente milhares de radiografias classificadas como normais ou com fracturas e aplica esse conhecimento aos novos exames. Esta técnica foi de resto já aplicada com sucesso no diagnóstico da retinopatia diabética (…) e cancro da pele[159]. Segundo o médico especialista, a técnica diagnóstica, que combina dados informáticos e pensamento clínico, é relevante também para a precisão da deteção das fraturas, na medida que a aumenta significativamente, quando comparada apenas com a análise humana *in* CARNEIRO, António, V., Inteligência Artificial em Saúde e os seus problemas, Revista Visão, 25.08.2018.

[160] COMISSÃO EUROPEIA. Comunicação sobre o *Plano Coordenado para a Inteligência Artificial*. COM/2018/795 final.

Europa (2020-2027)[161] e no *Programa Europa Digital (2021-2027).* Este último, financia projetos em cinco domínios fundamentais: supercomputação, inteligência artificial, cibersegurança, competências digitais avançadas, e ampla utilização das tecnologias digitais em toda a economia e sociedade[162].

Os dois programas, Horizonte Europa e Europa Digital (2021-2027)*,* são geridos pela mesma agência executiva e complementam-se, na medida em que o primeiro, financia as etapas iniciais da inovação; as atividades de I&D (incluindo testes preliminares e projetos piloto) e o segundo, possibilita a implantação tecnológica; financia projetos pilotos em grande escala em condições reais e permite usar os resultados da investigação para novas implantações.

Outro dado relevante é o facto do *Programa Europa Digital (2021-2027)*, viabilizar o *Plano de ação para a edução digital (2021-2027)*[163]*,* essencial à educação digital de qualidade, inclusiva e acessível na Europa. Nesse plano, serão desenvolvidas orientações éticas em matéria de IA, bem como recomendações sobre a utilização de dados no ensino e na aprendizagem, para os educadores.

Outro momento crucial para o tema em análise, foi a comunicação de 19 de fevereiro de 2020, durante a qual a Comissão Europeia apresentou *A European Strategy for Data* [164], na qual constam medidas políticas e de investimento, que visam habilitar a economia de dados para os próximos cinco anos.

Consciente dos desafios relacionados com a conectividade e o armazenamento**,** a cibersegurança[165] e a carência de competências digitais, a Comissão Europeia aponta uma estratégia para os ultrapassar, fazendo pleno uso do "quadro jurídico sólido – em termos de proteção de dados, direitos fundamentais, segurança e cibersegurança –, bem

[161] A Presidência alemã do Conselho da União Europeia (2º semestre de 2020), chegou a um acordo político provisório com os negociadores do Parlamento Europeu sobre a proposta de regulamento que estabelece o Horizonte Europa, o programa-quadro de investigação e inovação da UE para o período de 2021 a 2027.
[162] *Programa Europa Digital* - o Conselho e o Parlamento Europeu chegaram a um acordo provisório no dia 14.12.2020 sobre um *novo programa, o Europa Digital*, que promoverá a implantação em larga escala de tecnologias de ponta, como a inteligência artificial e a cibersegurança, a fim de impulsionar a transformação digital das sociedades e economias europeias. O programa decorrerá durante o período de vigência do Quadro Financeiro Plurianual (QFP) para 2021-2027, sendo dotado de um orçamento no montante de 7 588 milhões de euros**.**
[163] COM(2020) 624 Final.
[164] COM(2020) 66.
[165] A Comissão incumbiu a Agência da União Europeia para a Cibersegurança, ENISA, de preparar o esquema de certificação de cibersegurança da UE para redes 5G que ajudará a abordar os riscos relacionados com as vulnerabilidades técnicas das redes e a aumentar ainda mais a sua cibersegurança.

como no seu mercado interno, empresas competitivas de todas as dimensões e uma base industrial diversificada"[166].

A estratégia europeia de dados foi apresentada em simultâneo com a *Shaping Europe's Digital Future* e o *White Paper on Artificial Intelligence*[167]. Estes documentos complementam-se e são indispensáveis às pretensões da União Europeia de assumir um papel de liderança na economia dos dados.

A criação de um mercado único de dados, deve atender à conectividade, ao tratamento e ao armazenamento de dados, de modo a aumentar os repositórios de dados de qualidade disponíveis para utilização e reutilização, aumentar a capacidade computacional, bem como a cibersegurança. Além disso, terá de melhorar as suas estruturas de governação para manuseamento de dados[168].

Recorde-se que em 2015, a Comissão Europeia apresentou o *Mercado Único Digital*, um pacote legislativo que veio colmatar a ausência de instrumentos supraestaduais de proteção do cidadão, ajustados à realidade internacional. Um ano depois, foi publicado o Regulamento Geral de Proteção de Dados (RGPD), publicado em 27 de abril de 2016[169], a Diretiva de Cooperação Policial aprovada a 27 de abril de 2016[170], o Regulamento da Cibersegurança em 2017, e a proposta de Regulamento de Privacidade Eletrónica[171].

Em dezembro de 2020, a Comissão Europeia apresentou a proposta de regulamento do Mercado Único dos Serviços Digitais – *Digital Services Act (DAS)*[172] e a

[166] COM(2020) 66, p. 1.
[167] COM(2020) 65.
[168] COM(2020) 66, p. 1.
[169] JOUE. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27.04.2016.
[170] JOUE. Diretiva (UE) 2016/680, de 27.04.2016.
[171] COM(2017) 10final.
[172] Proposta de Regulamento do Parlamento Europeu e do Conselho sobre um Mercado Único de Serviços Digitais «Lei dos Serviços Digitais», COM(2020) 825final, 15.12.2020. Atualiza a Diretiva sobre o Comércio Eletrónico, Diretiva 2000/31/CE, de 08.06.2000.
O novo quadro proposto no DSA pretende reequilibrar os direitos e responsabilidades dos utilizadores, plataformas intermediárias e autoridades públicas e baseia-se nos valores europeus incluindo a liberdade de expressão e de informação (al. b) do artigo 26.º e al. e) do artigo 37.º), democracia (ponto (68) e (69) do preâmbulo) e igualdade e não discriminação (ponto (52), (63), (91) do preâmbulo, al. b) do artigo 26.º e al. e) do artigo 37.º). Por exemplo, as plataformas que atinjam mais de 10% da população da UE (45 milhões de utilizadores) serão consideradas como sendo de natureza sistémica e estarão sujeitas não apenas a obrigações específicas de controlo dos seus próprios riscos, nomeadamente regras para a remoção de bens, serviços ou conteúdos ilegais em linha, mas também a uma nova estrutura de supervisão. Este novo quadro de responsabilização propõe a existência de um conselho de Coordenadores de Serviços Digitais nacionais, com poderes especiais para a Comissão na supervisão de plataformas muito grandes, incluindo a capacidade de as sancionar diretamente.

proposta de regulamento sobre Mercados Digitais – *Digital Markets Act (DMA)*[173], propondo uma ambiciosa reforma do espaço digital, dando seguimento ao iniciado em 2015, mas com novas regras para todos os serviços digitais, incluindo redes sociais, mercados digitais e outras plataformas *online* que operam na União, visando preparar os Estados-membros para a era da digitalização, baseando-se em soluções digitais que dão prioridade à ação humana.

A ambição da União Europeia é liderar a transição digital[174]. Esse desiderato foi apresentado pela Comissão na comunicação intitulada «Construir o futuro digital da Europa», na qual observou também que as soluções digitais, tais como os sistemas de comunicações, a inteligência artificial ou as tecnologias quânticas, podem melhorar a nossa vida. Mas, acrescentou igualmente que,

> "os benefícios das tecnologias digitais não estão isentos de riscos, nem de custos. Os cidadãos sentem que já não controlam o que acontece aos seus dados pessoais e que são cada vez mais objeto de um número excessivo de solicitações artificiais. A ciberatividade mal-intencionada pode ameaçar o nosso bem-estar pessoal e desestabilizar as nossas infraestruturas críticas, para além de comprometer os nossos interesses mais vastos em matéria de segurança. Esta profunda transformação da sociedade apela a uma reflexão de fundo a todos os níveis sobre a melhor forma de a Europa responder a estes riscos e desafios. As dificuldades serão enormes, mas a Europa dispõe, inquestionavelmente, dos meios necessários para concretizar um futuro digital melhor para todos."

No início de 2020, a Europa foi desafiada pelo SARS-CoV-2, um novo coronavírus identificado pela primeira vez em Wuhan, China, a COVID-19, e que se transformou numa pandemia, reconhecida pela Organização Mundial de Saúde (OMS) no dia 11 de março de 2020. Nessa altura, a ciência já se mobilizava para acelerar, inovar e otimizar as soluções terapêuticas, que vieram a ser decisivas no controlo da pandemia.

A crise de saúde pública causada pela COVID-19, obrigou os Estados-membros a enfrentar um desafio sem precedentes com impactos nos seus sistemas de saúde, no seu modo de vida, na sua estabilidade económica e nos seus valores[175]. Em resposta, a União Europeia, assumindo que nenhum Estado-membro podia ser bem-sucedido agindo

---

[173] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector «Digital Markets Act», COM(2020) 842final,15.12.2020.
A proposta de DMA, vem no seguimento do Regulamento UE 2019/1150, de 20 de junho de 2019, e estabelece regras harmonizadas que definem e proíbem as práticas desleais dos *gatekeepers*, plataformas com um número igual ou superior a 45 milhões de utilizadores, como a Amazon, Apple, Facebook, Google e Microsoft, e fornece um mecanismo de aplicação baseado em investigações de mercado. O mesmo mecanismo garantirá que as obrigações estabelecidas no regulamento sejam mantidas em dia na realidade digital em constante evolução.
[174] COM(2020) 67final.
[175] JOUE. Recomendação (UE) 2020/518, da Comissão, de 8 de abril de 2020.

isoladamente e apresentou um conjunto de medidas integradas no *Espaço Europeu de Dados de Saúde.* Esta iniciativa visa reforçar o quadro da UE para a deteção e resposta a ameaças sanitárias transfronteiriças graves, bem como a consolidação dos papéis das agências existentes. Anunciou também, que numa segunda fase, serão criadas: uma *agência de investigação e desenvolvimento avançados no domínio biomédico* e *uma nova estratégia farmacêutica*, para analise da segurança da cadeia de abastecimento da Europa e garantia do acesso dos cidadãos a medicamentos seguros, a preços acessíveis e de alta qualidade.[176]

A resposta conjunta à pandemia levou a Comissão Europeia a criar relevantes instrumentos e ações na área da saúde pública, que são aqui meramente enumerados:

i) Regulamento (UE) 2020/1043 de 15 de julho de 2020, relativo à realização de ensaios clínicos com medicamentos para uso humano que contenham ou sejam constituídos por organismos geneticamente modificados destinados a tratar ou prevenir a doença do coronavírus (COVID-19) e ao fornecimento desses medicamentos
ii) Diretiva (UE) 2020/2020 do Conselho de 7 de dezembro de 2020, no que diz respeito a medidas temporárias relativas ao imposto sobre o valor acrescentado aplicável às vacinas contra a COVID-19 e aos dispositivos médicos para diagnóstico in vitro desta doença em resposta à pandemia de COVID-19.
iii) Comunicação da Comissão sobre as estratégias de vacinação contra a COVID-19 e a disponibilização das vacinas.
iv) Recomendação (UE) 2020/1632 do Conselho de 30 de outubro de 2020, sobre uma abordagem coordenada das restrições à liberdade de circulação em resposta à pandemia de COVID-19 no espaço Schengen [177].

Face à magnitude da crise, impunha-se uma resposta rápida e coordenada das instituições para a aquisição das vacinas à escala europeia, bem como o seu acesso por parte de todos os Estados-membros, configurando uma ação no domínio da saúde pública, uma ação conjunta onde os Estados-membros foram chamados a colaborar num verdadeiro espírito de solidariedade[178].

No âmbito deste especial contexto pandémico, surgiu a oportunidade das autoras, separadas por um oceano, se envolverem numa investigação bibliográfica, exploratória e utilizando o método hipotético-dedutivo, com o objetivo de analisar os desafios à proteção de dados pessoais derivados da aplicação da inteligência artificial, na União Europeia; o ecossistema industrial, mais concretamente a análise de custos e benefícios

[176] COM(2020) 690 final.
[177] EUR-LEX. Lista de documentos chave de saúde pública.
[178] JOUE. Recomendação (UE) 2020/518 da Comissão de 8 de abril de 2020.

de atribuição de patentes na área da saúde; o acesso a medicamentos inovadores e a sustentabilidade da indústria farmacêutica europeia.

Da investigação conclui-se, que relativamente aos dados de saúde e aos dados genéticos, o seu tratamento decorre em conformidade com o RGPD. Na prática, as instituições europeias têm desenvolvidos esforços no sentido de garantir os direitos fundamentais, num contexto crucial para a Ciência e para os cientistas, que no exercício das suas atividades de investigação, acedem a um grande volume de dados gerados, e com base nos megadados e no uso da IA, conseguem oferecer as tão necessárias inovações terapêuticas.

Podemos desde já observar, que o quadro desafiante provocado pela pandemia teve o mérito de impulsionar a criação de uma estrutura regulatória abrangente, que irá definir a melhor forma de a UE regular a IA de modo a impulsionar a inovação, as normas éticas e a confiança na tecnologia. O mesmo contexto, fez emergir o debate em torno do ecossistema industrial e das patentes na área da saúde, temática que é delineada por contornos jurídicos e civilizacionais.

1. A saúde pública no direito europeu

Desde as iniciais preocupações com a saúde dos trabalhadores na União Europeia, até ao atual nível de proteção de saúde de vigilância, alerta, combate contra as ameaças à saúde pública e incentivo à cooperação entre os Estados-membros, de modo a aumentar a complementaridade dos seus serviços de saúde nas regiões transfronteiriças[179], foi percorrido um longo e profundo itinerário. A intervenção da Comissão Europeia no âmbito da pandemia não pode ser entendida como um ato isolado. Com efeito, a União tem vindo a fazer um caminho de proteção da Saúde, embora ainda muito modesta quanto às suas competências nessa área.

A política de saúde da UE resultou das disposições em matéria de saúde e segurança, tendo-se, mais tarde, desenvolvido na sequência da livre circulação de pessoas e bens no mercado interno, contexto que exigia uma coordenação no domínio da saúde pública. Nesse sentido, podemos afirmar que a política europeia de saúde foi intentada em 1993, e é precursora de programas plurianuais de saúde pública subsequentes[180], a

[179] CAMPOS, António Correia de. Comentário ao artigo nº 168.º TFUE, in *Tratado de Lisboa,* 2012, p. 711.

[180] A avaliação desse primeiro programa concluiu que era necessária uma abordagem mais horizontal e interdisciplinar no futuro, para que a ação da UE conseguisse criar valor acrescentado. Esta abordagem foi acolhida na conceção dos programas subsequentes, ou seja, o Programa de Saúde Pública da UE 2003-

exemplo do atual "Programa EU4Health 2021-2027"[181], que irá investir 9,4 mil milhões de euros no financiamento dos Estados-membros, de organizações de saúde e de Organizações Não Governamentais.

Não obstante a ausência de uma base jurídica clara, a política de saúde pública tinha-se desenvolvido em várias áreas. Criou-se legislação em matéria de medicamentos em 1965, com o objetivo de regular a investigação, o fabrico de medicamentos e a harmonização dos procedimentos nacionais de autorização de medicamentos. Abrangia ainda as regras sobre a publicidade, a rotulagem e a distribuição. Em 1978, iniciaram-se os programas de investigação no campo da medicina e da saúde pública, tendo como objeto de estudo questões como o envelhecimento, os problemas de saúde relacionados com o ambiente e o estilo de vida, os riscos da radiação e a análise do genoma humano, com especial atenção para as principais doenças existentes na época[182].

Porém, é no Tratado de Maastricht (1992) que se consagra a base jurídica para a adoção de medidas de política de saúde, disposições que foram reforçadas no Tratado de Amesterdão (1997).

No âmbito do Tratado de Lisboa (2009), o artigo 168.º do Tratado sobre o Funcionamento da União Europeia (TFUE) reforça a cooperação entre a União, os Estados-membros e as organizações internacionais competentes no domínio da saúde pública. Segundo o Parlamento Europeu, são três os objetivos estratégicos de saúde pública prosseguidos pela União:

i) Promoção da saúde, prevenir doenças e promover estilos de vida saudáveis tomando medidas sobre as questões da nutrição, atividade física, consumo de álcool, tabaco e drogas, riscos ambientais e lesões. Importando lembrar que com o envelhecimento da população, as necessidades de saúde específicas dos idosos exigem mais atenção, inclusive tendo sido mais enfatizada a saúde mental nos últimos anos;

ii) Proteção dos cidadãos contra ameaças à saúde, melhorar a vigilância e a preparação para casos de epidemias e bioterrorismo e aumentar a capacidade de resposta aos novos desafios na área da saúde, designadamente as alterações climáticas;

2008, o Programa de Saúde 2009-2013 e o Terceiro Programa de Saúde 2014-2020 e atual programa UE pela Saúde (2021-2027).

[181] Os objetivos do *programa EU4Health 2021-2027* passam por: i) reforçar o grau de preparação da UE para as principais ameaças sanitárias transfronteiriças: constituir reservas de material médico para situações de crise; criar uma reserva de profissionais de saúde e de peritos que possam ser mobilizados para responder a crises sanitárias em toda a UE; aumentar a vigilância das ameaças sanitárias; ii) reforçar os sistemas de saúde para que possam enfrentar epidemias, bem como os desafios a longo prazo, ao estimular: a prevenção de doenças e a promoção da saúde numa população envelhecida; a transformação digital dos sistemas de saúde; o acesso aos cuidados de saúde para os grupos vulneráveis; disponibilizar e tornar acessíveis os medicamentos e os dispositivos médicos, defender a utilização prudente e eficiente dos agentes antimicrobianos, bem como promover a inovação médica e farmacêutica e o fabrico mais ecológico.

[182] PARLAMENTO EUROPEU. Fichas temáticas sobre a União Europeia, Saúde Pública 2021. https://www.europarl.europa.eu/factsheets/pt/sheet/49/public-health

iii) Apoio aos sistemas de saúde dinâmicos, ajudar os sistemas de saúde dos Estados-Membros a responder aos desafios colocados pelo envelhecimento das populações, pelas expectativas mais elevadas dos cidadãos e pela mobilidade de doentes e de profissionais da saúde e, assim, a ajudar os Estados-Membros a tornar os seus sistemas de saúde sustentáveis[183].

No presente, verifica-se que a melhoria da saúde pública, a prevenção das doenças e infeções humanas e a redução dos fatores de risco para a saúde física e mental, fazem parte da política da saúde da União (n.º 1 do artigo 168.º TFUE). Porém, a organização, a prestação e a gestão de serviços de saúde e de cuidados médicos, bem como a repartição dos recursos que lhes são afetados[184], é igualmente competência da União, mas é exercida em complemento das políticas nacionais e no respeito pelo princípio da subsidiariedade.

Ainda no plano europeu, o direito ao mais elevado padrão de saúde física e mental constitui um direito humano fundamental, tal como se extrai do artigo 35.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), que estatui

> «o direito de aceder à prevenção em matéria de saúde e de beneficiar de cuidados médicos, de acordo com as legislações e práticas nacionais. Na definição e execução de todas as políticas e ações da União é assegurado um elevado nível de proteção da saúde humana.»

Partindo deste enquadramento legal, a União Europeia enfrentou a pandemia de forma ímpar. Partiu-se do entendimento que só uma ação conjunta poderia dar uma resposta adequada. Com esse objetivo, a Presidente da Comissão Europeia, Ursula von der Leyen, assegurou, no âmbito da *Estratégia da UE para as vacinas contra a COVID 19*[185], a aquisição de mais de 1000 milhões de doses de vacinas, tendo posteriormente alocado as referidas doses a cada Estado-membro, de acordo com a sua população. Para tal, celebrou contratos com empresas fabricantes de vacinas, em nome de todos os Estados-membros, os designados *acordos prévios de aquisição*, com o intuito de "acelerar o desenvolvimento, o fabrico e a disponibilização de vacinas contra a COVID-19"[186].

No final de 2020, as vacinas contra a COVID-19 foram sendo disponibilizadas à medida que eram aprovadas pela Agência Europeia de Medicamentos (EMA). Assim, se pretendia garantir o acesso às vacinas em toda a UE, bem como distribuir de forma equitativa pelos países mais carenciados, tornando a vacina um bem público mundial. Essa distribuição estava assente em valores de universalidade, solidariedade e respeito

[183] PARLAMENTO EUROPEU. Fichas temáticas sobre a União Europeia, 2021.
[184]CAMPOS, António Correia de. Comentário ao artigo nº 168.º TFUE, in *Tratado de Lisboa,* 2012, p. 710.
[185]COM(2020) 245 final.
[186]SNS. Plano de Vacinação COBID-19, 3 de dezembro de 2020.

mútuo, em conformidade com o terceiro objetivo da Agenda de Desenvolvimento Sustentável 2030, das Nações Unidas[187]. Infelizmente as falhas na produção das vacinas e outras vicissitudes, impossibilitaram a concretização do plano de vacinação na União.

1.1.Organização e prestação de cuidados de saúde

O Tratado de Lisboa estipula que «na definição e execução de todas as políticas e ações da União será assegurado um elevado nível de proteção da saúde». Porém, a responsabilidade pela proteção da saúde e, em especial, pelos próprios sistemas de saúde continua a incumbir, em primeiro lugar, aos Estados-membros, de acordo com o nº 7 artigo 168.º TFUE.

Assim se justifica, que mesmo perante uma pandemia, cada Estado-membro tenha direito à aquisição de uma quantidade determinada de vacinas contra a COVID-19, durante um determinado período e a um determinado custo, parcialmente financiado pelo *Instrumento de Apoio de Emergência*. Assim se compreende que a Alemanha, a exemplo de outros países, já tenha adquirido autonomamente vacinas para a COVID19, e em Portugal há quem defenda a mesma prática. Ainda assim, a União partiu para esta ação concertadamente, seguindo atentamente a comunicação da Comissão Europeia sobre a «Preparação para as estratégias de vacinação contra a COVID-19 e a disponibilização das vacinas»[188], de 15 de outubro de 2020, foi facultado um pré-financiamento aos produtores de vacinas, a fim de acelerar o desenvolvimento e o fabrico de vacinas experimentais e garantir que os Estados-membros teriam acesso a essas vacinas nas melhores condições possíveis.

A Comissão celebrou acordos com vários produtores de vacinas em nome dos Estados-membros, adquirindo e/ou reservando o direito de adquirir doses de vacinas ao abrigo de acordos prévios de aquisição. Com esse objetivo foram celebrados contratos, nomeadamente com a AstraZeneca, a Sanofi-GSK e a Johnson&Johnson, que permitem comprar vacinas uma vez comprovada a sua segurança e eficácia. Em outubro de 2020, a Comissão celebrou acordos semelhantes com outros fabricantes de vacinas (CureVac, Moderna e BioNTech/Pfizer). Para mais, e tendo em vista a melhor coordenação dos procedimentos junto à Comissão Europeia, foi criado um *Steering Board*, no qual Portugal é representado pelo INFARMED - Autoridade Nacional do Medicamento e Produtos de Saúde, I. P.

[187] *Idem ibidem*.
[188] COM(2020) 680 final.

Portugal aderiu à aquisição de vacinas no âmbito do procedimento europeu centralizado. A Resolução do Conselho de Ministros n.º 64-A/2020 de 20 de agosto, consagrou uma autorização para a realização de despesa relativa à primeira fase dos procedimentos aquisitivos e, por intermédio do Despacho nº. 11737/2020, de 26 de novembro de 2020, emitido pelos Ministérios da Defesa Nacional, da Administração Interna e da Saúde, foi constituída uma *task force* para a elaboração do «Plano de vacinação contra a COVID-19 em Portugal», integrada por um núcleo de coordenação e por órgãos, serviços e organismos de apoio técnico das áreas acima citadas. O Plano inclui a estratégia de vacinação, assegurando a logística do armazenamento e a distribuição das vacinas, garantindo o registo eletrónico da respetiva administração e da vigilância de eventuais reações adversas e promovendo uma comunicação transparente com a população sobre a importância da vacinação.

2. A relevância da inteligência artificial no contexto pandémico

O contexto pandémico veio provar que é imperioso "dispor de tecnologias ligadas à IA e de tecnologias conexas no domínio do reconhecimento remoto ou biométrico, como as aplicações de rastreio, enquanto nova forma de lidar com a COVID-19 e com eventuais crises sanitárias e de saúde pública que se apresentem no futuro, atendendo, simultaneamente, à necessidade de proteger os direitos fundamentais, o direito à vida privada e os dados pessoais (…)"[189].

Podemos então concluir que o cenário pandémico provocado pela COVID-19, tornou as inovações tecnológicas na área da saúde ainda mais relevantes para a sociedade[190].

Reforça-se, no entanto, que em face da COVID-19, exigia-se uma abordagem europeia comum para a salvaguarda dos direitos fundamentais, tal como foi assumido pela Comissão:

> "uma vez que as medidas tomadas em determinados países, tais como a monitorização de indivíduos através da geolocalização, a utilização da tecnologia para classificar o nível de risco sanitário dos indivíduos e a centralização de dados sensíveis, suscitam questões do ponto de vista de vários direitos e liberdades fundamentais garantidos na ordem jurídica da UE, incluindo o direito à privacidade e o direito à proteção dos dados pessoais. Em todos os casos, nos termos da Carta dos Direitos Fundamentais da União, as restrições ao exercício dos direitos e liberdades fundamentais nela reconhecidos devem ser justificadas e proporcionadas. Tais restrições devem, nomeadamente, ser temporárias, ou seja,

[189]PARLAMENTO EUROPEU. Relatório sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial, 2 de outubro 2020.
[190] INPI. *Importância das patentes na área da saúde (medicamentos e vacinas)*, abril de 2020.

> limitar-se ao estritamente necessário para combater a crise e não continuar a existir, sem uma justificação adequada, após o termo da crise." [considerando 23] [191].

A Medicina, assim como todas as demais áreas do conhecimento relacionadas com a saúde, exige a padronização e a validação dos dados e de informações, se possível, ao nível universal. E, nessa medida, a aplicação da IA apresenta-se como uma tecnologia indispensável. É essa a mensagem da Presidente da Comissão Europeia no discurso pronunciado na apresentação do *"Masters of Digital 2021"*[192].

As palavras de Ursula von der Leyen expressaram confiança nos inúmeros benefícios da aplicação da IA. Sendo hoje, comumente aceite na Europa que "à medida que a tecnologia digital se torna um elemento cada vez mais central de todos os aspetos da vida das pessoas, é preciso que estas possam confiar nela"[193].

Ou seja, a fiabilidade é uma condição prévia para a sua aceitação.

Mark Coeckelbergh, no seu recente livro *AI ETHICS*, sublinha o impacto generalizado da IA na sociedade, embora muitas vezes, de forma invisível:

> "Given the exponential growth of computer power, the availability of (big) data due to social media and the massive use of billons of smartphones, and fast mobile networks, AI, especially machine learning, has made significant progress. This has enabled algorithms to take over many of our activities, including planning, speech, face recognition, and decision making. AI has applications in many domains, including transport, marketing, health care, finance and insurance, security and the military, science, education, office work and personal assistance (e.g., Google Duplex1), entertainment, the arts (e.g., music retrieval and composition), agriculture, and of course manufacturing."[194]

Em suma, a União pretende fazer avançar os progressos científicos, preservando a liderança tecnológica, desde que as novas tecnologias estejam ao serviço de todos os cidadãos europeus, melhorando as suas vidas e respeitando simultaneamente os seus direitos.

2.1. Os principais postulados éticos da inteligência artificial

Os princípios éticos vão além dos aspetos legais *soft ethics*, exigindo-se um agir baseado em valores, em direitos e na responsabilidade *hard ethics*. Trata-se de uma ética capaz de moldar a legislação, designadamente o Regulamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), no sentido do seu aperfeiçoamento.

---

[191] JOUE. Recomendação (UE) 2020/518, da Comissão, de 8 de abril de 2020.
[192] Discurso da Presidente da Comissão Europeia no evento de apresentação do "Masters of Digital 2021", 4 de fevereiro de 2021.
[193] COM(2020) 65 final, p. 1.
[194] COECKELBERGH, Mark. *AI ETHICS*, 2020, p. 3.

Os princípios e os direitos humanos fundamentais estão ancorados na dignidade da pessoa humana e constituem um porto de abrigo, um referencial ao qual já não se pode abdicar[195]. Estes referenciais têm vindo a iluminar o iter traçado pela União Europeia, desde a Estratégia Europeia para a Inteligência Artificial (2018), à publicação do Livro Branco para a Inteligência Artificial e a Estratégia para a Proteção de Dados (2020), até ao Espaço Europeu de Dados de Saúde (2020).

No *Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*, refere-se que "a supervisão humana contribui para garantir que um sistema de IA não põe em causa a autonomia humana nem produz outros efeitos negativos. O objetivo de uma IA fiável, ética e centrada no ser humano só pode ser alcançado por meio da garantia de um envolvimento adequado dos seres humanos em aplicações de IA de alto risco[196]. Afirma ainda que,

> "Embora a IA possa ter muitas utilizações positivas, nomeadamente tornando os produtos e os processos mais seguros, também pode ter utilizações negativas. Essas utilizações negativas podem ser materiais (segurança e saúde das pessoas, incluindo a perda de vida, danos materiais) e imateriais 12 (perda de privacidade, limitações ao direito à liberdade de expressão, dignidade humana, discriminação, por exemplo, no acesso ao emprego) e podem estar relacionadas com uma grande variedade de riscos. O quadro regulamentar deverá incidir na forma de minimizar os vários riscos de potenciais danos, em especial os mais significativos"[197].

Para garantir a correta aplicação da IA, a Comissão Europeia criou em 2018, o Grupo de Peritos de alto nível sobre a IA (GPAN IA), composto por especialistas, provenientes da academia, das empresas e da sociedade civil, com a missão de apoiar a implementação da estratégia europeia de inteligência artificial. No mesmo ano, o GPAN IA apresentou o primeiro projeto de orientações éticas, muito influenciado pelo Grupo Europeu de Ética para as Ciências e as Novas Tecnologias e pela Agência dos Direitos Fundamentais. Foi igualmente criado em 2018, a *Aliança Europeia para a IA*, uma plataforma aberta que tem por objetivo reunir contributos para o grupo de peritos então criado.[198]

Em março de 2019, o GPAN IA apresentou o documento revisto, texto que foi bem acolhido pelos Estados-membros, no qual defende que uma «IA de confiança» só é alcançada se respeitar os valores europeus, que se baseiam no respeito pela dignidade

---

[195] CALDEIRA, Cristina, «O impacto ético e jurídico da aplicação das novas tecnologias na área da saúde» 2020, p. 222-253.
[196] COM(2020) 65, p.22.
[197] COM(2020) 65, p. 11e12.
[198] Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial. *Orientações éticas para uma inteligência artificial*, junho 2018, p. 6.

humana, fundamento axiológico da União Europeia, na liberdade, na democracia, na igualdade, no Estado de direito e no respeito pelos direitos humanos, tal como prevê o Tratado da União Europeia (TUE), no artigo 2.º e a CDFUE. Estes direitos, princípios e valores devem ser observados ao longo do ciclo de vida do sistema de IA, atendendo a três componentes cruciais: conformidade com a legislação; respeito dos princípios éticos e; robustez.

Concomitante com a UE, a Organização para a Cooperação e Desenvolvimento Económico (OCDE) enunciou um conjunto de princípios[199] que devem nortear a aplicação da IA em benefício das pessoas e do planeta[200].

A OCDE defende que os princípios se complementam e devem ser considerados como um todo. Estes princípios orientam os países da OCDE[201] e do G20, bem como a Bulgária, o Chipre, a Croácia e Malta, Estados-membros da União Europeia. Por último, a Albânia, a Andorra, a Armênia, o Azerbaijão, a Bósnia e Herzegovina, a Geórgia, o Liechtenstein, a Macedónia do Norte, a Moldávia, o Mónaco, o Montenegro, o San Marino, a Sérvia e a Ucrânia foram incluídos através do Conselho da Europa, que aprovou uma Recomendação CM/Rec(2020)1 do Comité de Ministros aos Estados Membros, sobre o impacto dos sistemas algorítmicos sobre os direitos humanos, a 8 de abril de 2020.

Em suma, inúmeros países passaram a exigir dos seus governos, uma cumplicidade com os *Princípios da OCDE*, que em muito se aproximam dos princípios apresentados pelo GPAN IA. Sem impor uma hierarquia, o GPAN IA identificou sete princípios que se complementam[202] e onde se incluem aspetos sistémicos, individuais e

---

[199] A OCDE defende um conjunto de princípios: crescimento inclusivo; desenvolvimento inclusivo; desenvolvimento sustentável e bem-estar; valores focados nos seres humanos e na justiça; transparência e explicabilidade; robustez; segurança e proteção e prestação de contas.

[200] OCDE. «Recomendação do Conselho da Inteligência Artificial», aprovada em 22 de maio de 2019.

[201] A OCDE integra países como a Alemanha, Áustria, Austrália, Bélgica, Canadá, Chile, Coreia do Sul, Dinamarca, Eslováquia, Eslovénia, Espanha, EUA, Estónia, Finlândia, França, Grécia, Hungria, Irlanda, Islândia, Israel, Itália, Japão, Letónia, Lituânia, Luxemburgo, México, Nova Zelândia, Noruega, Países Baixos, Polónia, Portugal, Reino Unido, República Checa, Suécia, Suíça e Turquia, tendo a Recomendação do Conselho da OCDE sobre Inteligência Artificial sido também subscrita pela Argentina, Colômbia, Costa Rica, Peru e Roménia, além de pelo Brasil, como referimos no início

[202] "1 - Ação e supervisão humanas (Incluindo os direitos fundamentais, a ação humana e a supervisão humana); 2 - Solidez técnica e segurança (Incluindo a resiliência perante ataques e a segurança, os planos de recurso e a segurança geral, a exatidão, a fiabilidade e a reprodutibilidade); 3 - Privacidade e governação dos dados (Incluindo o respeito da privacidade, a qualidade e a integridade dos dados e o acesso aos dados); 4 - Transparência (Incluindo a rastreabilidade, a explicabilidade e a comunicação); 5 -Diversidade, não discriminação e equidade (Incluindo a prevenção de enviesamentos injustos, a acessibilidade e a conceção universal e a participação das partes interessadas); 6 -Bem-estar societal e ambiental (Incluindo a sustentabilidade e o respeito do ambiente, o impacto social, a sociedade e a democracia); 7 - Responsabilização (Incluindo a auditabilidade, a minimização e a comunicação dos impactos negativos, as

sociais. Destes, destaca-se a essencialidade das decisões finais serem humanas, sempre que atinjam direitos fundamentais. Mas, é na Declaração Universal dos Direitos Humanos que vamos encontrar os alicerces éticos, uma norma moral universal, a fundamentação humana dos valores, tal como nos ensina Norberto Bobbio,

> "[…] la manifestazione dell'unica prova con cui un sistema di valori può essere considerato umanamente fondato e quindi riconosciuto: e questa prova è il consenso generale circa la sua validità. I giusnaturalisti avrebbero parlato di 'consensus omnium gentium' o 'humani generis'. [até porque] "Non so se ci si rende conto sino a che punto la Dichiarazione universale rappresenti un fatto nuovo nella storia, in quanto per la prima volta nella storia un sistema di principi fondamentali della condotta umana è stato liberamente ed espressamente accettato, attraverso i loro rispettivi governi, dalla maggior parte degli uomini viventi sulla terra. Con questa dichiarazione un sistema di valori è (per la prima volta nella storia) universale, non di princÍpio ma di fatto, in quanto il consenso ulla sua validità e sulla sua idoneità a reggere le sorti della comunità futura di tutti gli uomini è stato esplicitamente dichiarato" [203],[204].

Convidados a testar a lista de avaliação criada pelo GPAN IA[205], cada Estado membro pode intervir comunicando informações sobre a forma de melhorar o ecossistema IA. Paralelamente a Comissão organizou atividades de sensibilização, permitindo ao GPAN IA apresentar as orientações para a IA junto dos Estados membros e em especial do setor da indústria e dos serviços.

Em 2020, por efeito da *Aliança Europeia da Inteligência Artificial* e da AI4EU[206], atualizaram-se as orientações, que devem constituir a base do quadro jurídico operacional para o desenvolvimento da IA e de políticas públicas, contribuindo dessa forma para a construção de um quadro de cooperação global que assegure a fiabilidade da IA e que garanta a integridade dos direitos humanos e fundamentais.

Consciente do impacto que a IA pode ter na sociedade, bem como das suas implicações humanas e éticas, a Comissão Europeia defende a melhor utilização de

---

soluções de compromisso e as vias de recurso)", *in* Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial (GPAN IA)*, Orientações éticas para uma inteligência artificial*, 2019, p. 6.

[203] "[...] a manifestação da única prova pela qual um sistema de valores pode ser considerado fundado humanamente e, portanto, reconhecido: esta prova é o consenso sobre a sua validade. Os jusnaturalistas falariam de "consenso omnium gentium" ou "humani generis". [até porque] "Não sei se percebemos até que ponto a Declaração Universal representa um novo facto na história, uma vez que, pela primeira vez na história, um sistema de princípios fundamentais de conduta humana foi livre e expressamente aceite, através dos respetivos governos, pela maioria dos homens vivos na Terra. Com esta declaração, um sistema de valores é (pela primeira vez na história) universal, não de princípio, mas de facto, uma vez que o consenso sobre a sua validade e a sua adequação ao destino da futura comunidade de todos os homens foi explicitamente declarado" (tradução livre).

[204] MASSENO, Manuel D. «Das Consequências Jurídicas da Adesão do Brasil aos Princípios da OCDE para a Inteligência Artificial, Especialmente em Matéria de Proteção de Dados», 2020, p. 114.

[205] Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial*, Orientações éticas para uma inteligência artificial*, p. 32 a 40.

[206] Plataforma lançada em janeiro de 2019, que reúne algoritmos, ferramentas, conjuntos de dados e serviços para ajudar as organizações a aplicarem soluções de inteligência artificial.

grandes volumes de dados para a inovação[207]. É com esse objetivo que apoia uma abordagem regulamentar orientada para o investimento na IA, que regule os riscos associados a determinadas utilizações desta nova tecnologia[208] e que se baseie nos valores europeus e nos direitos fundamentais dos cidadãos europeus, como a dignidade humana e a proteção da privacidade[209]. A proposta deverá integrar a definição de aplicações de alto risco, a regulação dos fornecedores de sistemas de IA, a vigilância pós-mercado de IA, a avaliação da conformidade das aplicações de IA de alto risco, entre outras matérias.

Do que vimos anteriormente, a profunda transformação da sociedade, se, por um lado, faz crescer a tensão entre a evolução tecnológica e a regulação, por outro lado, faz apelo a novos compromissos éticos[210], na medida em que se tornou claro que a UA pretende aumentar a confiança numa inteligência artificial centrada no ser humano e baseada em princípios[211].

Existe consenso quanto à criação de um quadro regulamentar para a IA, entre as instituições europeias. O Parlamento Europeu aprovou uma Resolução com a iniciativa legislativa «Regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas»[212], na qual reforça a necessidade de um enquadramento legal eficaz e harmonizado para a IA, baseado no direito da União, na CDFUE e no direito internacional em matéria de direitos humanos, aplicável, em particular, às tecnologias de alto risco, a fim de estabelecer normas iguais em toda a União e de proteger eficazmente os valores da União.

Em suma, as disposições do direito europeu continuarão a aplicar-se com as atualizações necessárias à transformação digital[213], forçando um enquadramento legal europeu da IA, proposta que se tornará pública ao longo do primeiro semestre de 2021, durante a Presidência Portuguesa do Conselho da União Europeia, e, que se espera, que Portugal venha a dar um contributo numa matéria tão relevante.

---

[207] COM(2020) 65, p. 1.
[208] COM(2020) 65, p. 1.
[209] COM(2020) 65, p. 2.
[210] ANTUNES, Henrique Sousa, *Direito e Inteligência Artificial*, 2020, p.7.
[211] COM(2019)168 final.
[212] PARLAMENTO EUROPEU. Resolução que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas, 20 de outubro de 2020.
[213] COM(2020) 65, p. 18.

3. Comentários sobre a proposta de um quadro regulamentar europeu para a inteligência artificial

Os desafios da aplicação da IA para a privacidade e para a segurança, são enormes, sendo o campo jurídico desafiado continuamente pelo caráter disruptivo da IA. É incontestável que se assiste a um desafio contínuo, que se agudiza na medida em que as tecnologias se tornam mais invasivas, subtis, tornando-se necessário definir limites éticos que possam assegurar o espaço vital e o mínimo existencial das populações afetadas.

O quadro regulamentar europeu da IA deve ir além da componente legal, devendo também reforçar a componente ética e oferecer confiança[214]. Nesta matéria o Parlamento Europeu defende que,

> "só pode ser conseguida com base num quadro regulamentar de ética por definição e desde a conceção que garanta que toda e qualquer IA posta em funcionamento respeite integralmente os Tratados, a Carta e o direito derivado da União; considera que tal abordagem deve ser consentânea com o princípio da precaução que orienta a legislação da União e deve estar no cerne de qualquer quadro regulamentar para a IA(…) Espera que a Comissão integre uma abordagem ética sólida na proposta legislativa (…) no seguimento do Livro Branco sobre a Inteligência Artificial, nomeadamente em matéria de segurança, responsabilidade e direitos fundamentais, que maximize as oportunidades e minimize os riscos das tecnologias de IA."

O enquadramento legal da IA deve ser baseado no risco. A relação do ser humano com as chamadas novas tecnologias, traduz um ponto de inflexão em todas as áreas, com especial impacto ao nível da subjetividade, da responsabilidade, da memória, da privacidade e da autonomia de cada ser humano. Desde a moral, a ética, a ciência, a economia ao Direito, estão a ser efetivadas alterações profundas. A esse propósito, Parlamento Europeu enumerou "uma lista dos setores de alto risco e das utilizações ou finalidades que encerram um risco de violação dos direitos humanos e fundamentais e das regras de segurança como o emprego, a educação, saúde, transportes, energia, o setor público (asilo, migração, controlos nas fronteiras, sistema judicial e serviços da segurança social), a defesa e segurança, finanças, banca e seguros"[215].

Particular atenção merece a área da saúde e em especial a matéria de segurança e da responsabilidade que são específicos dos cuidados de saúde. Nessa medida deverão ser consideradas as implicações jurídicas dos sistemas de IA que fornecem informações

[214] PARLAMENTO EUROPEU. Resolução que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas, 20 de outubro de 2020.

[215] PARLAMENTO EUROPEU. Resolução que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas, 20 de outubro de 2020.

médicas especializadas aos médicos, sistemas de IA que fornecem informação médica diretamente aos doentes e sistemas de IA que executam diretamente tarefas terapêuticas. Defendemos, no entanto, que os aspetos já abrangidos pela legislação horizontal ou setorial existente, a exemplo dos dispositivos médicos, continuarão a ser regidos por esta legislação, eventualmente carecerão de atualização.

Exemplificando algumas riscos no setor da saúde, se por um lado, uma falha no sistema de marcação de horários de consultas num hospital não constitui um risco, já os tratamentos e procedimentos médicos podem oferecer um alto risco[216], que é ainda mais acentuado quando por via da aplicação de IA se possa pôr em causa a privacidade do paciente, a confidencialidade dos dados sensíveis (informação de saúde,[217] e informação genética[218]), podendo inclusivo, resultar numa lesão, morte ou outros danos materiais e imateriais de relevo. A realidade do presente, força o legislador a regular por exemplo quem pode aceder às bases de dados dos pacientes, por quanto tempo, bem como o controlo dos acessos. Estas são as razões que estão na base das reservas relativas à aplicação da inteligência artificial e à sua utilização para obtenção de informação de saúde.

A OCDE e várias organizações internacionais têm alertado para esses riscos. A Comissão, nas suas várias comunicações, o Comité Europeu para a Proteção de Dados, nas suas diretivas, e a Comissão Nacional de Proteção de Dados, lançaram alertas e esforçam-se por nos apresentar uma direção, que passa pela necessidade de uma avaliação de impacto sobre a proteção de dados, bem como a segurança do tratamento, para além

---

[216] PARLAMENTO EUROPEU. Resolução que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas, 20 de outubro de 2020.

[217] Entendemos por informação de saúde, «todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar» (artigo 2.º da Lei n.º 12/2005, de 26 de janeiro, Informação genética pessoal e informação de saúde, atualizada pela Lei n.º 26/2016, de 22 de agosto).

[218] «1. A informação genética é a informação de saúde que verse as características hereditárias de uma ou de várias pessoas, aparentadas entre si ou com características comuns daquele tipo, excluindo-se desta definição a informação derivada de testes de parentesco ou estudos de zigotia em gémeos, dos estudos de identificação genética para fins criminais, bem como do estudo das mutações genéticas somáticas no cancro. 2 - A informação genética pode ser resultado da realização de testes genéticos por meios de biologia molecular, mas também de testes citogenéticos, bioquímicos, fisiológicos ou imagiológicos, ou da simples recolha de informação familiar, registada sob a forma de uma árvore familiar ou outra, cada um dos quais pode, por si só, enunciar o estatuto genético de uma pessoa e seus familiares. 3 - A informação genética reveste natureza médica apenas quando se destina a ser utilizada nas prestações de cuidados ou tratamentos de saúde, no contexto da confirmação ou exclusão de um diagnóstico clínico, no contexto de diagnóstico pré-natal ou diagnóstico pré-implantatório ou no da farmacogenética, excluindo-se, pois, a informação de testes preditivos para predisposições a doenças comuns e pré-sintomáticos para doenças monogénicas» (artigo 6.º Lei n.º 12/2005, de 26 de janeiro, Informação genética pessoal e informação de saúde, atualizada pela Lei n.º 26/2016, de 28 de agosto).

da observância dos princípios da necessidade e da proporcionalidade. A este propósito, não nos afastamos do ponto essencial da proteção dos dados, aspeto fundamental na construção de um sistema protetivo, não somente tecnicamente adequado quanto juridicamente seguro e comprometido com a responsabilidade e a solidariedade.

3.1. Equilíbrio entre a segurança e a privacidade

É inegável que há um alinhamento entre os Estados-membros da União, quanto ao modo como enfrentam o problema da proteção de dados, em especial no que afeta à segurança e à transmissibilidade[219]. A esse propósito, a *Estratégia europeia para os dados* assume a confiança como elemento essencial de uma economia dos dados, ágil, atrativa, segura e dinâmica, capaz de melhorar as decisões e a vida de todos os seus cidadãos. Nessa matéria, a UE coopera com os países que perfilam os mesmos valores, mas também com outros intervenientes mundiais, que partilhem uma abordagem assente nas regras e valores defendidos pela UE e dentro do espírito de uma concorrência equitativa[220].

A necessidade de promover a segurança no tão desejado regresso à normalidade no pós-pandemia, não poderá, no entanto, ser baseada na restrição dos nossos direitos humanos e fundamentais. Nessa conformidade, o tratamento dos dados pessoais deve observar o respeito pelo conteúdo essencial dos direitos afetados. De referir, que a proteção de dados pessoais, constitui-se como um direito humano, que é posto à prova por via da aplicação de novas tecnologias (IA e robótica), bem como pela ciência de dados (big data). Porém, "o direito à proteção de dados pessoais não é absoluto (e) deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade." [Considerando 4 RGPD].

Atendendo a que tanto os dados relativos à saúde como os dados genéticos, são integrados nas categorias especiais de dados pessoais e por essa razão proíbe-se o seu tratamento, tal como decorre do n.º 1 do artigo 9.º do RGPD, e no Considerando 51 RGPD:

> "merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente

[219] CALDEIRA, C. e SARLET, G. «O consentimento informado e a proteção de dados pessoais de saúde na Internet – uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana», 2020, p. 260.
[220] COM(2020) 65, p. 10.

regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas."

No plano interno, a Lei n.º 12/2005, de 26 de janeiro, que regula a Informação Genética Pessoal e Informação de Saúde, atualizada pela Lei n.º 26/2016, de 22 de agosto, promoveu uma mudança paradigmática relativamente à titularidade dos dados pessoais de saúde. No seu artigo 3.º, o legislador adota o conceito de **"**informação de saúde[221]", em detrimento dos dados relativos à saúde, e consagra essa informação como sendo "propriedade" da pessoa a quem os dados dizem respeito.

No plano do direito europeu, mantêm-se os «dados relativos à saúde», definidos como dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde que revelam informações sobre o seu estado de saúde (nº 15 artigo 4.º RGPD). Com relevância para o tratamento de dados sensíveis, importa incluir os «dados genéticos», que são definidos pelo legislador europeu, como dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa (nº 15 artigo 4.º RGPD).

Em síntese, é razoável defender que o legislador, ao apresentar um quadro regulamentar para a IA, mantenha inalteradas as designações previstas no RGPD. Por sua vez, não funcionando os sistemas de IA à margem da lei, a sua aplicação deve não só ser coerente com a legislação, assegurando eventuais danos decorrentes da sua aplicação, como respeitar os princípios éticos.

Contudo, torna-se pertinente analisar as garantias que devem ser prestadas pelos profissionais de saúde e pelas unidades do sistema de saúde, relativamente à segurança da informação, quando em causa está o tratamento de dados de saúde, ensaios clínicos, medicina preventiva, diagnóstico médico, a prestação de cuidados ou tratamentos médicos e a gestão dos serviços de saúde.[222] À luz do RGPD, o tratamento desses dados são lícitos desde que efetuados por um profissional de saúde sujeito a sigilo médico ou

[221] O legislador define «informação de saúde» como um conceito macro onde cabem todas as informações relativas à saúde de uma pessoa, especificamente os dados registados nos processos clínicos, os resultados de análises e de outros exames subsidiários, das intervenções e dos diagnósticos, que são manejadas pelos profissionais de saúde na sua relação assistencial (Lei n.º 12/2005, de 26 de janeiro, que regula a Informação genética pessoal e informação de saúde, atualizada pela Lei n.º 26/2016, de 22/08).

[222] CALDEIRA, C. e SARLET, G. «O consentimento informado e a proteção de dados pessoais de saúde na Internet – uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana», 2020, p. 247.

por outra pessoa obrigada a segredo profissional de saúde e, desde que estejam garantidas medidas de segurança da informação (artigo 32.º). Por sua vez, o dever de sigilo é aplicável a todos os titulares de órgãos e trabalhadores que, no contexto do acompanhamento financeiro ou fiscalização da atividade de prestação de cuidados de saúde, tenham acesso a dados relativos à saúde[223].

O consentimento do titular dos dados constitui um outro fundamento legítimo para o tratamento dos dados pessoais sensíveis previstos por lei, quer no RGPD, quer num outro ato de direito da União ou de um Estado-membro, tal como se refere no considerando 40 do RGPD. Trata-se de uma pedra angular, na medida em que traça os novos contornos tanto da liberdade quanto da autonomia tendo por base a responsabilidade.

Quando o tratamento de dados pessoais se fundamenta na monitorização de uma epidemia, bem como da sua propagação ou, em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana, será igualmente lícito o tratamento dos dados de saúde e de dados genéticos, mesmo sem consentimento do titular dos dados, tal como se extrai do considerando 46 do RGPD:

> "quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários(…)".

As derrogações ao nº 1 do artigo 9.º do RGPD encontram-se previstas nº 2 do mesmo artigo. Da leitura da *g*) do nº 2 do artigo 9.º e do considerando 54, consolida-se a certeza que as atividades de tratamento sobre a saúde são autorizadas por motivos de interesse público, não devendo esses dados serem tratados para outros fins e de acesso por parte de terceiros, a exemplo de companhias de seguros e bancos. Porém, admite-se poder incluir o tratamento de dados de saúde em tempo de pandemia, com recurso às tecnologias digitais através da criação da aplicação móvel[224], para o acesso a informações sobre o nível de circulação do vírus.

---

[223] CALDEIRA, C. e SARLET, G. «O consentimento informado e a proteção de dados pessoais de saúde na Internet – uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana», 2020, p. 239 e 240.

[224] Face a estes argumentos, aceita-se uma limitação da privacidade desde que:

1. A finalidade do tratamento seja clara; assumimos que a finalidade é a primeira justificação para a realização de um tratamento de dados. Acompanhamento quem defende que a finalidade constitui

Esta informação, sobre a qual a Comissão Nacional de Proteção de Dados (CNPD) já se pronunciou, deverá permitir uma melhor avaliação da eficácia das medidas físicas de distanciamento e confinamento, bem como uma melhor informação para o combate da COVID19. De qualquer modo, a CNPD exigiu critérios claros para diferenciar as várias aplicações de IA quando se trata de saber se são ou não «de alto risco». Porém, mesmo que uma aplicação de IA não seja qualificada como de alto risco, continua a estar inteiramente sujeita a regras da UE já existentes[225].

Os cidadãos devem ser claramente informados quando interagem com um sistema de IA e não com um ser humano. De acordo com o RGPD, os responsáveis pelo tratamento devem, aquando da recolha dos dados pessoais, fornecer aos titulares dos dados as informações suplementares necessárias para assegurar um tratamento equitativo e transparente da existência de tomadas de decisões automatizadas e de certas informações adicionais" (alínea f) do n.º 2 do artigo 13.º)[226].

Partindo do elevado risco que certas aplicações de IA representam para os cidadãos e para a nossa sociedade, será necessário uma avaliação prévia e objetiva da conformidade, prevista no artigo 35.º do RGPD, de modo a garantir o cumprimento de alguns dos requisitos obrigatórios às aplicações de alto risco[227], nomeadamente a segurança do tratamento dos dados (artigo 32.º RGPD), tal como foi mencionado anteriormente. Por sua vez, o controlo *ex post* deve ser facilitado por documentação adequada relativa à aplicação de IA em causa[228].

---

a trave mestra fundamental do regime jurídico da proteção de dados pessoais. Defendemos quer toda a recolha de dados sensíveis deve ter uma finalidade determinada explícita e legitima;

2. O armazenamento da informação seja justificado. Exigimos uma adequação, pertinência e a limitação do tratamento desses dados às finalidades essenciais (minimização dos dados);
3. A Conservação apenas durante o tempo necessário às finalidades para as quais são tratadas (limitação da conservação);
4. Exigência da aplicação de medidas técnicas e organizativas, de modo a que promova a salvaguarda dos direitos e liberdades do titular dos dados;
5. Õ tratamento dessa informação sensível se faça em segurança não permitindo o tratamento não autorizado (integridade e confidencialidade).
6. Seja igualmente defendido o direito ao apagamento dos dados pessoais, quando sejam superadas as razões que levaram ao seu tratamento;
7. Atribuição da responsabilidade pelo tratamento da informação;
8. Já não aceitamos, que as atividades de tratamento de dados constituam uma porta aberta para a discriminação, para a criação de perfis, incompatíveis com a finalidade ou a minimização dos princípios básicos, mas orientadores, previstos no art 5.º do RGPD. E como tal não abdicamos da Licitude, da Lealdade e da transparência do tratamento dos dados pessoais e em especial dos dados de saúde.

[225] COM(2020) 65, p. 19.
[226] COM(2020) 65, p. 22.
[227] COM(2020) 65, p. 25.
[228] COM(2020) 65, p. 26.

Em síntese e revisitados os principais postulados éticos que permitem a interpretação das regras jurídicas, importa salientar que é na tutela internacional dos direitos humanos e fundamentais, que se alicerçam os imperativos éticos geralmente formulados nos documentos de referência sobre a IA. Por seu lado, a ética carece da coercibilidade que só o direito garante[229], mas as normas de IA devem respeitar os princípios éticos, e ser coerentes com a legislação, de modo a sancionar eventuais danos decorrentes da sua aplicação. Por último, a IA deve consagrar o respeito pelos direitos fundamentais dos cidadãos, aumentando as suas capacidades e não as subtraindo, em todas as suas aplicações.

4. A construção de uma União Europeia da saúde

Na conferência dedicada à "Saúde Digital 2020-UE em Movimento", organizada pela Presidência alemã do Conselho da UE, no dia 11 de novembro de 2020, anunciou-se a intenção da União trabalhar em conjunto, para uma utilização dos dados de saúde de forma segura e orientada para os doentes. Reafirmou-se a vontade de colaborar no domínio dos dados de saúde em todo o espaço europeu, para uma melhor saúde, melhor investigação e melhor desenho das políticas de saúde. Nessa mesma data, e no seguimento da *Estratégia em Matéria de Dados*, foi lançado a criação do *Espaço Europeu de Dados de Saúde*, com propostas que vão no sentido de reforçar a preparação e a resposta a crises sanitárias[230].

A construção de uma União Europeia para a saúde encontra a base jurídica no artigo 168.º do TFUE, que tutela um quadro regulamentar abrangente aplicável aos produtos e às tecnologias na área da medicina (medicamentos, dispositivos médicos e substâncias de origem humana), direitos dos doentes nos cuidados de saúde transfronteiriços e às ameaças sanitárias transfronteiriças graves. E, tal como o afirmamos anteriormente, embora os Estados-membros sejam responsáveis pelo funcionamento dos seus sistemas de saúde, existem domínios específicos em que a UE pode legislar e outros em que a Comissão pode apoiar os esforços dos Estados-membros.

---

[229] ANTUNES, Henrique Sousa, *Direito e Inteligência Artificial*, 2020, p.7.

[230] A *União Europeia de Saúde* inclui propostas como: reforçar a coordenação a nível da UE na eventualidade de ameaças sanitárias com dimensão transfronteiriça; rever os mandatos do Centro Europeu de Prevenção e Controlo das Doenças e da Agência Europeia de Medicamentos, a fim de reforçar a vigilância, a análise científica e as orientações antes e durante uma crise e criar uma nova agência da UE para a preparação biomédica. Disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_pt

O espaço europeu de dados de saúde permitirá o acesso aos dados de saúde ao abrigo de uma governação fidedigna e regras claras e apoiará a livre circulação de serviços digitais de saúde. Até 2025, os pacientes de todos os Estados-membros irão poder partilhar os seus dados com profissionais de saúde à sua escolha, quando viajam para o estrangeiro.

Numa segunda fase, a Comissão Europeia pretende criar uma *Agência de investigação e desenvolvimento avançados no domínio biomédico*, bem como *Uma Nova Estratégia Farmacêutica* que analisará a segurança da cadeia de abastecimento da Europa e garantirá o acesso dos cidadãos a medicamentos seguros, a preços acessíveis e de alta qualidade.[231]

A proposta regulamentar de criação do programa de ação da União no domínio da saúde para o período 2021-2027, prevê que o *Programa UE pela Saúde* contribua para a Carta dos Direitos Fundamentais da União Europeia, na medida em que irá melhorar o acesso a cuidados de saúde preventivos, e o direito a beneficiar de tratamento médico, nas condições estabelecidas pelas legislações e práticas nacionais.

O novo programa está também em consonância com o objetivo da Carta dos Direitos Fundamentais da União Europeia, ao assegurar um elevado nível de proteção da saúde humana na definição e execução de todas as políticas e ações da União[232].

As diversas iniciativas elencadas neste ponto, apresentam-se pertinentes ao tema em estudo, tornando obrigatória uma reflexão mais adensada sobre a ética na ciência, sobre as tecnologias computacionais inteligentes e a saúde, na sua relação com o direito fundamental à proteção de dados, os direitos humanos e o direito industrial.

5. A convergência entre o direito de propriedade intelectual e os direitos humanos

Vários doutrinadores sublinharam a capacidade de a sociedade organizar e sistematizar dados e informações relativos à saúde. Cristina CALDEIRA e Márcia FERNANDES citam Floridi para observar que "a capacidade da civilização humana em registar, organizar e gerir dados e informações, possibilitou o registo histórico, ou seja, ditou a própria História.

No presente, vive-se a quarta grande revolução do processo civilizacional humano, a exemplo de outras experienciadas, como foi a revolução de Copérnico, de

[231] COM(2020) 690 final, p. 8.
[232] COM(2020) 405 final, p. 8.

Gutemberg e de Freud. A informação está presente em tudo o que corresponde ao ser humano, alterando ontologicamente a nossa existência[233].

A pandemia exigiu a sistematização da recolha, do armazenamento, da utilização de dados e informações de saúde. Exigiu por outro lado também o incremento global do conhecimento na área da saúde, a mobilização de centros de investigação, laboratórios, universidades e empresas. Esta partilha de informação sensível e de conhecimento, num esforço de convergência sem precedentes da comunidade científica global, potenciou formas inovadoras de responder às necessidades em termos de diagnóstico, vacinas e soluções terapêuticas de difícil obtenção com metodologias tradicionais.

Esta crescente sistematização de dados e de informações em saúde humana, teve como preocupação o respeito pelos Direitos Humanos Fundamentais e de Personalidade, destacando-se os direitos de privacidade e os deveres de confidencialidade. O mesmo respeito deve ser observado quando se tutela a produção científica através do Direito de Propriedade Intelectual. Vale destacar que, em função da pandemia, jamais se viu tamanha profusão de dados e tampouco foi produzida de uma única vez tanta informação acerca desse tema, gerando um verdadeiro novo eldorado para a indústria farmacêutica.

O regime internacional dos direitos da propriedade intelectual e os Direitos Humanos Fundamentais evoluíram de uma forma independente. Porém, com o alargamento do âmbito de aplicação das patentes a áreas relacionadas com as necessidades básicas, como é a saúde, e em especial num contexto pandémico, a ligação entre os dois domínios torna-se óbvia e direta, merecendo uma reflexão sobre o direito à saúde e a tutela de patentes na área da saúde (medicamentos e vacinas).

As *patentes* constituem monopólios que a sociedade está disposta a aceitar, por assumir que os benefícios das inovações na área da saúde serão superiores ao preço de monopólio que terão de suportar. Nessa medida e tal como defende a Organização Mundial da Saúde *in* «*Public Health, Innovation and Intellectual Property Rights*», justifica-se a atribuição da exclusividade por meio da patente por via dos *incentivos ao investimento em I&D*; pelo potencial de *transação de tecnologia especializada*; pela *divulgação de informações técnicas à sociedade* e pela capacidade inovadora que apresenta, podendo

[233]CALDEIRA, Cristina e FERNANDES, Márcia. «A partilha de dados pessoais sensíveis, dados epidemiológicos (COVID-19) e genéticos: aspectos jurídicos e bioéticos na perspetiva da União Europeia, Portugal e Brasil», 2020, p. 324.

ter acesso a *financiamento de capital de risco*, mediante o seu capital intelectual protegido[234].

Perante a catástrofe sanitária mundial, corria-se contra o tempo em busca de duas conquistas fundamentais: vacinas e aplicações móveis de vigilância epidemiológica, interoperáveis, que recorrendo à IA e ao uso do big data, fosse capaz de criar redes de vigilância epidemiológica em toda a Europa. O desenvolvimento e a disponibilização de vacinas eficazes e seguras apresentavam-se como elementos essenciais para o controlo da pandemia, o que ditou um grande investimento na Ciência em ambiente colaborativo - *collaborative research and development* (R&D), na designação inglesa).

Defendemos, que o ambiente colaborativo e o sucesso da Ciência é fruto de uma harmonização internacional da propriedade industrial, alcançada mediante tratados, tais como a *Convenção de Paris para a Proteção da Propriedade Industrial (1883, com várias revisões);* o *Tratado de Cooperação em Matéria de Patentes - PCT (1970)*[235] e o *Acordo TRIPS (1994),* onde se estabeleceu uma proteção mínima para os direitos industriais.

Numa breve referência aos instrumentos internacionais sobre a proteção da propriedade industrial, infere-se que o pretendido é o incentivo à inovação, ao mesmo tempo, que se instituíram flexibilidades às disposições consagradas nos tratados, em prol da proteção dos direitos humanos, através da salvaguarda da saúde pública, do acesso a medicamentos e vacinas, sobretudo por parte dos países em desenvolvimento.

A *Convenção de Paris para a Proteção da Propriedade Industrial* afirma o *princípio de solidariedade* entre os Estados unionistas e faz prevalecer o *direito unionista* sobre os seus membros, por meio do qual se estabelece uma proteção mínima para os direitos da propriedade industrial. À luz desta Convenção, a apresentação de um pedido de patente de invenção num Estado Contratante confere, dentro de certo prazo, um direito de prioridades para apresentação do pedido nos outros Estados contratantes (arts 4.º bis; 6.º/3 e 4.º/A/1 da Convenção de Paris). Em síntese, o direito unionista edifica-se com base em três princípios fundamentais: o *princípio da assimilação ou do tratamento nacional*; o *princípio da independência* e o *princípio do direito da prioridade unionista*[236].

[234] OMS. «Public Health, Innovation and Intellectual Property Rights», 2006, p.19, 20 e 21.
[235] WIPO/OMPI. Perguntas e Respostas sobre o PCT.
[236] MACHADO, João Baptista. *Lições de Direito Internacional Privado*, 2017, p. 386-392.

O *Tratado de Cooperação em matéria de Patentes* (PCT), é o instrumento multilateral da Organização Mundial da Propriedade Intelectual (OMPI/WIPO) [237], que integra mais de 150 Estados Contratantes, através do qual é permitido solicitar a proteção de uma invenção através de patente simultaneamente num grande número de países, depositando um único pedido de patente internacional.

O PCT expressa a vontade dos Estados contratantes em contribuir,

> "to foster and accelerate the economic development of developing countries through the adoption of measures designed to increase the efficiency of their legal systems, whether national or regional, instituted for the protection of inventions by providing easily accessible information on the availability of technological solutions applicable to their special needs and by facilitating access to the ever expanding volume of modern technology." [238]

O Acordo sobre os Aspetos dos Direitos de Propriedade Intelectual relacionadas com o comércio (TRIPS)[239], veio reforçar a proteção da propriedade intelectual. O TRIPS assenta em 2 princípios gerais fundamentais: *o princípio do tratamento nacional* (artigo 3.º, nº 1) e o do *tratamento da nação mais favorecida* (artigo 4.º). Nos termos do Acordo TRIPS, todas as invenções devem poder ser protegidas por uma patente durante 20 anos, quer se trate de uma *patente de produto* um medicamento, ou a uma *patente de processo*, onde se inclui o método de produção de um medicamento. Para que, quer o produto, quer o processo, seja patenteável, a invenção tem de ser *nova*, constituir uma *atividade inventiva* e ter *aplicabilidade industrial*.

Ao instituir um sistema de proteção da Propriedade Intelectual, o Acordo TRIPS[240] fá-lo à margem do sistema anteriormente existente, ou seja, à margem da Organização Mundial da Propriedade Intelectual (OMPI). Em síntese, o TRIPS contém um sistema que diverge do sistema da OMPI, quanto aos destinatários, ao conteúdo, à prevenção e à resolução de litígios, entre outros.

O Acordo TRIPS protege as patentes farmacêuticas no artigo 33.º, o qual determina que a duração da proteção auferida pela patente não terminará antes do termo de um período de vinte anos calculado a partir da data de depósito, isto é, da data da

---

[237] WIPO/OMPI. Perguntas e Respostas sobre o PCT.
[238] WIPO/OMPI. Thirty-Sixth Series of Meetings Geneva, September 24 to October 3, 2001, p. 4.
[239] O Acordo TRIPS prevê normas mínimas para a proteção de patentes, marcas comerciais, direitos autorais e outros direitos de propriedade intelectual.
[240] Em Portugal, à data de aplicação do TRIPS (1 de janeiro de 1996), a matéria da propriedade industrial encontrava-se regulada, em termos de direito interno, pelo Código da Propriedade Industrial aprovado pelo Decreto-Lei n.º 16/95, de 24 de janeiro, para entrar em vigor em 1 de junho de 1995(6), que substituíra o anterior Código da Propriedade Industrial, aprovado pelo Decreto n.º 30679, de 24 de agosto de 1940. No presente, a propriedade industrial é regulada pelo Decreto-Lei nº 110/2018, de 10 de dezembro, que a prova o novo Código da Propriedade Intelectual, transpondo as Diretivas (UE)2015/2436 e (UE) 2016/943.

apresentação do respetivo pedido. O Acordo consagra também uma flexibilidade na aplicação das suas disposições, consoante os interesses e as circunstâncias nacionais, mas salvaguardando-se a primazia da proteção da saúde pública.

Em rigor, o desfecho favorável das negociações multilaterais do *Uruguay Round* (1986/1994), realizadas no âmbito da Organização Mundial do Comércio (OMC), que levou ao Acordo sobre os Aspetos dos Direitos de Propriedade Intelectual relacionadas com o comércio-TRIPS (1994), só foi possível pela valorização dada à *dimensão ética* enquanto decorriam as discussões sobre patentes de medicamentos. Pode-se mesmo afirmar, que foram as distorções do comércio internacional que forçaram a convergência para a formalização de um regime de combate aos obstáculos à internacionalização da ciência. A inclusão do Acordo TRIPS nas negociações multilaterais no âmbito *do Uruguay Round*, permitiu superar muitos obstáculos. Foi por iniciativa dos países em desenvolvimento, que as questões referentes à saúde pública inseridas no Acordo TRIPS, culminaram na *Declaração de Doha sobre o Acordo TRIPS e a Saúde Pública* (2001).

A *Declaração de Doha da OMC sobre o Acordo TRIPS e Saúde Pública*, vincula os temas de propriedade intelectual e da saúde pública, e estabelece a "primazia" das políticas de saúde pública sobre os direitos de propriedade intelectual. Nessa matéria, a Declaração representou um marco adicional na histórica das patentes farmacêuticas. Na prática, tendo em consideração as assimetrias entre países desenvolvidos e os países em vias de desenvolvimento, determina a Declaração de Doha[241] que os países em desenvolvimento ou em estágio de subdesenvolvimento recorram a acordos comerciais que lhes permitam importar os medicamentos em tempo útil.

Atualmente, a eficácia do Acordo TRIPS é dificultada por acordos assinados fora do âmbito da OMC. Estes acordos são conhecidos como *TRIPS-plus.* Procedeu-se à celebração de *Acordos TRIPS-plus* entre os EUA e os países da América Latina, acordos preferenciais de comércio, destacando especificamente o conteúdo *TRIPS*-plus das regras de proteção à propriedade intelectual contidas nos acordos. Essas regras ampliam e aprofundam o padrão mínimo obrigatório do TRIPS, produzindo efeitos importantes em políticas públicas vitais para o desenvolvimento socioeconómico desses países, dificultando o acesso a medicamentos junto aos Estados signatários.

No plano europeu, a *Convenção sobre a Patente Europeia* (1973, revista em 1978 e 2000) estabelece um processo unificado de concessão de patente para um ou mais

[241]CULLET, Philippe. «Patents and medicines: the relationship between TRIPS and the human right to health», 2003, 152.

Estados Contratantes, dando origem a vários direitos de propriedade intelectual independentes entre si[242].

Por último, o *Projeto de Criação de Patente Europeia com Efeito Unitário* que se apresentou sob a forma de regulamento, o Regulamento (UE) nº 1257/2012, que consagra um regime de cooperação reforçada (previsto no artigo 20.º do Tratado da União Europeia e os artigos n.º 326.º e seguintes do Tratado sobre o Funcionamento da União (TFUE), que corresponde a um efeito jurídico novo da patente europeia à qual nos referimos anteriormente, e não a um novo título jurídico unitário, contudo não foi ainda aprovada. A sua aprovação permitiria produzir efeitos em todo o território da União Europeia. Em complemento, o Acordo relativo ao Tribunal Unificado de Patentes (ATIP), aprovado em 2013, mas ainda não entrou em vigor, ainda reforça as condições para o acesso à patente unificada.

Em fevereiro de 2020, O Tribunal Constitucional Alemão, em sede de fiscalização preventiva publicada a 20 de março de 2020, considerou inconstitucional o Ato de Aprovação do Acordo sobre um Tribunal Unificado de Patentes, em virtude do Parlamento alemão não o ter aprovado com a maioria de dois terços. Tratava-se de uma aprovação relevante na medida em eu se transfere poderes soberanos sobre matéria de propriedade industrial para o Tribunal Unificado de Patentes. A 26 de novembro de 2020, o Parlamento alemão aprovou a ratificação por mais de dois terços de deputados[243].

A patente unitária foi colocada de novo na agenda política da União por Francisca Van Dunem, Ministra da Justiça de Portugal, aquando da primeira iniciativa da Presidência Portuguesa, intitulada: "A Metamorfose da Propriedade Intelectual na Era da Transição Digital"[244]. O sistema da patente unitária simplificará a conceção de patentes na União Europeia e criará um balcão único para as empresas, simplificando substancialmente a concessão de patentes na União Europeia[245].

[242]PINHEIRO, Luís de Lima. *Direito Internacional Privado*, Volume II, 2018, p. 630.
[243] BUNDESVERFASSUNGSGARICHT, Processo n.º 2-BvR 739/17, de 13 de fevereiro de 2020. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-020.html
[244]PRESIDÊNCIA PORTUGUESA DO CONSELHO DA UNIÃO EUROPEIA. "The Intelellectual Property metamorphosis in the Age of Digital Transition", 11 de fevereiro de 2021.
[245] COM(2020) 760 final, p. 5.

6. O ecossistema industrial e a tutela da inovação: os direitos industriais

No plano europeu, a promoção da inovação e da criatividade, bem como o acesso ao conhecimento e à informação, são tutelados através da criação de direitos europeus de propriedade intelectual, previstos no artigo 118.º do TFUE. Desse modo, o legislador europeu pretende assegurar uma proteção uniforme desses direitos em toda a União e incentivar a invenção[246]. Na prática, os direitos de propriedade intelectual são títulos exclusivos predominantemente disciplinados por regulamentos e a consagração europeia dos títulos baseia-se no "primado da livre circulação de produtos e serviços no seio do espaço da UE"[247].

Em 2020, a Comissão Europeia definiu *uma nova estratégia industrial para a Europa*[248], na qual demonstrou o empenho da União na investigação e na implantação de tecnologias em domínios como a IA, a tecnologia 5G, a análise de dados e metadados.

Sendo a Europa considerada o "berço da indústria"[249], pretende agora liderar o ecossistema industrial, contribuindo com as novas tecnologias emergentes para a sustentabilidade e a viabilidade da base industrial europeia.

Na mesma comunicação, a Comissão Europeia afirmou a importância da política de propriedade intelectual para o reforço da soberania da Europa no domínio da tecnologia e para as condições de concorrência equitativas à escala mundial. Para tal, a Comissão Europeia apelou a políticas inteligentes em matéria de propriedade intelectual[250], que garantam os ativos intangíveis, com especial destaque para os ativos industriais (as patentes) e determinem o valor de mercado, bem como a competitividade das empresas.

Em termos conceituais, a propriedade intelectual, na sua dimensão industrial, é definida pela Convenção da *Organização Mundial da* Propriedade Intelectual (OMPI/WIPO)[251] como:

> "a soma dos direitos relativos (…) às invenções em todos os domínios da atividade humana, às descobertas científicas, aos desenhos e modelos industriais, às marcas industriais, comerciais e de serviço, bem como às firmas comerciais e denominações

[246] PARLAMENTO EUROPEU. Relatório sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial, 2020.
[247] MARQUES, Remédio. Comentário ao artigo nº 118.º TFUE in *Tratado de Lisboa*, 2012.
[248] COM(2020)102, p.4.
[249] COM(2020)102, p.2.
[250] COM(2020)102, p.6.
[251] A OMPI, atualizada na versão de Estocolmo (1967) e por força do TRIPS /OMC (1994), celebrada no âmbito das Nações Unidas, integra a Convenção de Paris (1883), o primeiro acordo internacional relativo à Propriedade Intelectual para a Proteção da Propriedade Industrial (CUP). Integra ainda a Convenção da União de Berna (1886), relativa à proteção das obras literárias e artísticas.

comerciais, à proteção contra a concorrência desleal e todos os outros direitos inerentes à atividade intelectual nos domínios industrial, científico, literário e artístico".

A tutela dos direitos industriais visa contribuir para a promoção da inovação tecnológica, a transferência e difusão da tecnologia e o bem-estar social e económico. São estes os objetivos que norteiam várias convenções e acordos internacionais, desde a Convenção de Paris para a Proteção da Propriedade Industrial (1883) ao Acordo sobre os Aspetos dos Direitos de Propriedade Intelectual relacionadas com o comércio-TRIPS (1994), em vigor.

O "Direito Industrial" ou "Direito da Propriedade Industrial" na designação tradicional adotada pelo legislador português, encontra-se previsto no Decreto-Lei n.º 110/2018, de 10 de dezembro, o Código da Propriedade Industrial, (doravante designado CPI), que cobre dois grandes domínios:

i) a tutela da inovação (técnica ou estética), incluindo o regime das Patentes de Invenção, dos Modelos de Utilidade, das topografias dos Produtos Semicondutores, dos Direitos de obtenção Vegetal, bem como dos Desenhos ou Modelos;

ii) a proteção dos sinais distintivos do comércio, nomeadamente das Marcas, dos Logótipos, das Denominações de Origem e Indicações Geográficas, bem como, em certo sentido, das Firmas e das próprias Recompensas**.**

Estas duas categorias de direitos industriais, envolvem a atribuição de direitos exclusivos de utilização de determinados bens imateriais, relativos à inovação ou à diferenciação empresarial e, as duas categorias proíbem todos as demais do uso desses bens. Contudo, apresentam diferenças quanto à sua função e ao regime. Assim,

> "enquanto os direitos relativos à tutela da inovação visam incentivar a criatividade nos domínios da técnica e da estética industrial (através da atribuição de exclusivos temporários de exploração), os grupos de sinais distintivos destinam-se a ordenar a concorrência no mercado (mediante a atribuição de sinais privativos de identificação dos produtos, dos serviços ou das empresas, de duração indefinidamente renovável.[252]"

O artigo 50.º do CPI, refere que "podem ser objeto de patente as invenções novas, implicando atividade inventiva, se forem suscetíveis de aplicação industrial, mesmo quando incidam sobre um produto composto de matéria biológica, ou que contenha matéria biológica, ou sobre um processo que permita produzir, tratar ou utilizar matéria biológica" (n.º 1). Assim, podem obter-se patentes para quaisquer invenções, quer se trate

[252] SILVA, Pedro Sousa e. *Direito Industrial*, 2020, p. 15 e 16.

de produtos ou processos, em todos os domínios da tecnologia, desde que essas invenções respeitem o que se estabelece no número anterior" (n.º 2). Podem igualmente ser objeto de patente os processos novos de obtenção de produtos, substâncias ou composições já conhecidos" (nº 3).

A flexibilização atribuída às disposições previstas no CPI, reflete-se no ordenamento português, em matéria de *esgotamento da tutela* conferida ao titular do direito industrial (artigo 104.º CPI) e na *concessão de licenças obrigatórias* (artigos 108.º e 112º CPI). Ao abrigo da flexibilização de disposições consagradas no CPI, o titular de uma patente pode ser obrigado a conceder uma licença para a exploração da respetiva invenção por motivo de interesse público (art. 111.º CPI) [253]., quando «(…) o início, o aumento ou a generalização da exploração da invenção, ou a melhoria das condições em que tal exploração se realizar, sejam de primordial importância para a saúde pública ou para a defesa nacional».

A necessidade de uma eventual postura coerciva tem estado na ordem do dia, em virtude do incumprimento dos contratos por parte das empresas farmacêuticas na entrega de vacinas COVID19.

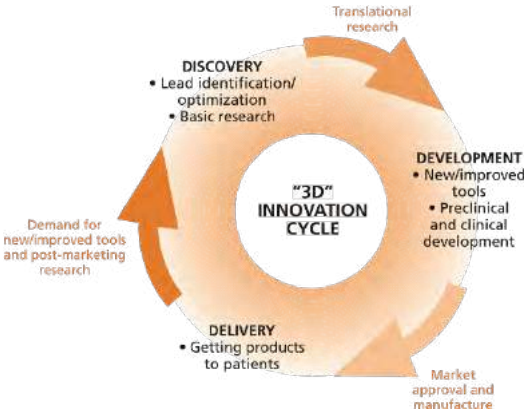
Ainda assim, a Comissão Europeia tem privilegiando o caminho da colaboração, agindo excecionalmente em sentido contrário, quando adotou a proibição das empresas farmacêuticas exportarem vacinas para fora da União Europeia.

7. O papel da indústria farmacêutica: equilíbrio e equacionamento entre custos e benefícios de atribuição de uma patente

A indústria farmacêutica desempenha um papel relevante na sociedade, através da produção e da comercialização de produtos que interferem diretamente com a saúde. Mas, o setor da indústria farmacêutica enfrenta desafios relacionados com os ciclos de inovação, por constituírem processos morosos e muitos exigentes financeiramente (fig. 1), verificando-se com frequência a celebração de parcerias público-privadas (PPP), com Universidades e outras entidades públicas. Nesaa matéria, a União Europeia está claramente em desvantagem face aos EUA, Japão e China, facilmente verificável pelo número de patentes apresentados por estes países.

[253] São os organismos nacionais ou regionais administradores de patentes, os responsáveis pela concessão das patentes na chamada fase nacional. Em Portugal, o processo de obtenção de patente, é da competência do Instituto Nacional de Propriedade Industrial. Por sua vez, a autorização de introdução no mercado (AIM) para a comercialização do medicamento é da competência da INFARMED. Passa ainda por um processo administrativo de fixação de um preço máximo de venda.

Fig. 1 Innovation Cycle



Fonte: OMS 2006, p. 22

A interpretação da fig. 1 permite-nos salientar que o setor das tecnologias da saúde (medicamentos, vacinas e dispositivos médicos), dependem dos direitos de propriedade industrial, nomeadamente através de patentes, para defender e assegurar os seus ativos. A competição na indústria farmacêutica é assim impulsionada pelo conhecimento científico, e pela tutela das invenções. E, como já afirmamos, a patente[254] constitui um título que confere um direito exclusivo de exploração de um invento, título que se justifica pelo investimento financeiro que é efetuado em I&D[255]. A proteção dos direitos industriais opera-se por meio de um requerimento de patente: internacional, europeia e nacional, sendo atribuída uma tutela legítima quando a invenção reúna três requisitos: novidade[256], atividade inventiva[257] e aplicação industrial[258].

[254] O processo de obtenção da patente de medicamento ou de processo, em Portugal é da competência do Instituto Nacional de Propriedade Industrial. Por sua vez, a autorização de introdução no mercado (AIM) para a comercialização do medicamento é da competência da INFARMED. Passa ainda por um processo administrativo de fixação de um preço máximo de venda.

[255] A necessidade de grandes investimentos e o risco dos mesmos tem determinado a criação de parcerias. A *Innovative Medicine Initiative (IMI)* é uma parceria público privada entre uma empresa comum à União Europeia, representada pela Comissão, e a Federação Europeia das Associações e Indústrias Farmacêuticas, para a investigação na área da saúde, que se desenvolveu no âmbito programa-quadro de pesquisa e inovação - Horizonte 2020. O principal objetivo é acelerar o desenvolvimento de medicamentos com objetivos específicos, como: aumentando da taxa de sucesso de ensaios clínicos de novos medicamentos e vacinas e desenvolver novos marcadores biológicos para diagnosticar doenças e avaliar tratamentos.

[256] O conceito de novidade implica que a invenção não está compreendida no estado da técnica (artigo 54º, n.º 1, do CPI). Por sua vez, o estado da técnica é constituído por tudo o que, dentro ou fora do País, foi tornado acessível ao público antes da data do pedido de patente, por descrição escrita ou oral, utilização ou qualquer outro meio (artigo 55º, n.º 1, do CPI), incluindo o conteúdo de pedidos de patente e modelos de utilidade requeridos em data anterior à do pedido de patente mesmo não publicados (artigo 55º, n.º 2, do CPI).

[257] Considera-se que uma invenção implica atividade inventiva, se, para um perito na especialidade, não resultar ou não for dedutível, de maneira evidente, a partir do estado da técnica (artigo 54º, n.º 2, do CPI).

[258] Considera-se que uma invenção é suscetível de aplicação industrial se o seu objeto puder ser fabricado ou utilizado em qualquer género de indústria ou na agricultura (artigo 54º, n.º 4, do CPI).

A atribuição da patente a uma empresa farmacêutica, visa garantir a lealdade da concorrência, pela atribuição de direitos privativos sobre os diversos processos técnicos de produção de um medicamento. Ou seja, as patentes proporcionam aos seus titulares os meios jurídicos para impedir que outros reproduzam, utilizem ou vendam novas invenções, por 20 anos, e sob reserva de um conjunto de exceções.

Reforçamos, que as patentes constituem monopólios que a sociedade está disposta a aceitar, mas o equilíbrio e o equacionamento entre os custos e os benefícios de atribuição de uma patente dependem do grau de desenvolvimento dos países. Esta posição foi defendida pela Organização Mundial da Saúde (OMS), segundo a qual:

> Intellectual property rights have an important role to play in stimulating innovation in health-care products in countries where financial and technological capacities exist, and in relation to products for which profitable markets exist. In developing countries, the fact that a patent can be obtained may contribute nothing or little to innovation if the market is too small or scientific and technological capability inadequate. In the absence of effective differential and discounted prices, patents may contribute to increasing the price of medicines needed by poor people in those countries. Although the balance of costs and benefits of patents will vary between countries, according to their level of development and scientific and technological infrastructure, the flexibility built into the TRIPS agreement allows countries to find a balance more appropriate to the circumstances of each country[259].

No recente estudo sobre a «Importância das patentes na área da saúde (medicamentos e vacinas)», publicado em abril de 2020, pelo INPI - Instituto Nacional de Propriedade Industrial, observa-se que o atual cenário pandémico de COVID-19 tornou as inovações tecnológicas na área da saúde ainda mais relevantes para a sociedade[260]. A saúde é um bem jurídico elevado à categoria de direito fundamental, plasmado no artigo 64.º da Constituição da República Portuguesa de 1976. Aí se encontra vertido não só um direito à proteção da saúde, mas também um dever de todos de promover e defender a saúde (n.º 1, 2ª parte), falamos de saúde pública.

Por fim, torna-se imperioso recordar que a atual conjuntura colocou por terra as posições acirradas numa perspetiva unicamente voltada para a economia, gerando forçosamente uma abordagem ancorada na solidariedade, na responsabilidade e, sobretudo na sustentabilidade

[259] OMS. «Public Health, Innovation and Intellectual Property Rights», 2006, p. 22.
[260] INPI. «Importância das patentes na área da saúde (medicamentos e vacinas)», abril de 2020.

7.1. As patentes farmacêuticas e os prazos especiais de proteção

Tal como o sinalizamos anteriormente, a proteção por patente tem a duração máxima de 20 anos (artigo 100.º CPI), podendo ser estendida por mais cinco anos, mediante determinadas condições, através de um certificado complementar de proteção (CCP)[261], instrumento que que vem ganhando cada vez importância no domínio da indústria farmacêutica. Estes prazos especiais são justificados segundo Inês AGAPITO, porque,

> "o período de vigência efetiva do direito de exclusivo conferido pela patente é muito inferior ao prazo legalmente consagrado. De facto, entre o momento em que uma empresa farmacêutica pede o registo de uma patente para uma invenção químico-farmacêutica e o momento em que pode comercializar essa invenção sob a forma de medicamento, para o que carece de uma autorização de introdução no mercado (AIM), decorre um intervalo de tempo que ronda os 10 anos. Assim se torna evidente que o direito de exclusivo conferido pela patente sofre, neste sector, uma redução significativa. Daqui decorrem alguns problemas. Por um lado, verifica-se que, neste aspeto, a indústria farmacêutica encontra-se em desvantagem face às demais indústrias produtivas que não estão sujeitas a qualquer limitação ou controlo prévio para explorar comercialmente os seus produtos. Por outro lado, vendo reduzido o período de exploração exclusiva dos seus produtos, as empresas farmacêuticas podem deparar-se com dificuldades em remunerar ou, sequer, amortizar os avultados investimentos feitos, o que poderá levar ao desinvestimento na área da investigação e desenvolvimento (I&D) de novos medicamentos, por falta de recursos."[262].

Quando a patente atinge o limite de vigência, "cai" no domínio público, ou seja, a invenção deixa de estar protegida e, a partir dessa data, qualquer entidade pode explorar essa mesma invenção. Esta limitação temporal incentiva as empresas a introduzir os medicamentos no mercado o mais rapidamente possível e a desenvolver, de uma forma contínua, medicamentos inovadores.

A tutela do direito industrial através de patentes ou de certificado complementar de proteção é atribuída ao «medicamento de referência ou original»[263]. Os «medicamentos genéricos»[264], que proporcionam aos doentes o acesso a um preço mais baixo, reduzindo

---

[261] O Certificado de Proteção para Medicamentos encontra-se previsto no Regulamento (UE) 2019/933 Do Parlamento Europeu e do Conselho de 20 de maio de 2019 que alterou o Regulamento (CE) n.º 469/2009, introduzindo algumas modificações a este regime, mais concretamente, introduziu exceções (ou waivers).

[262] AGAPITO, Inês. «O Certificado Complementar de Protecção para medicamentos», 2015.

[263] «Medicamento de referência», medicamento que foi autorizado com base em documentação completa, incluindo resultados de ensaios farmacêuticos, pré-clínicos e clínicos, segundo o artigo 3.º, n.º 1, *al* ii) do Decreto-Lei n.º 176/2006, atualizado pelo Decreto-Lei n.º 112/2019, de 16 de agosto. O presente decreto-lei marca uma profunda mudança no sector do medicamento, designadamente nas áreas do fabrico, controlo da qualidade, segurança e eficácia, introdução no mercado e comercialização dos medicamentos para uso humano.

[264] «Medicamento genérico», medicamento com a mesma composição qualitativa e quantitativa em substâncias activas, a mesma forma farmacêutica e cuja bioequivalência com o medicamento de referência haja sido demonstrada por estudos de biodisponibilidade apropriados (artigo 3.º, nº 1, *al* vv do Decreto-Lei n.º 176/2006, atualizado pelo Decreto-Lei n.º 112/2019, de 16 de agosto).

também as despesas do Sistema Nacional de Saúde, surgem na fase de caducidade/extinção da tutela do medicamente original, acrescida da dilação de um CCP.

Em Portugal, constata-se que a entrada dos medicamentos genéricos ocorre em momento muito tardio, em virtude dos titulares de patente, em particular de um medicamento de referência se socorrerem de vários instrumentos legais para retardarem a entrada de medicamentos genéricos no mercado. O objetivo é restringir a concorrência e prorrogar o monopólio legal outorgado por esse direito de propriedade industrial. O fundamento utilizado pelas empresas produtoras de medicamentos inovadores prende-se com o grande investimento/risco realizado e por se tratar de uma atividade relativamente à qual está subjacente um esforço intelectual do inventor.

Os argumentos acima produzidos levam-nos a compreender a dicotomia existente entre as empresas produtoras de medicamentos de referência e as empresas produtoras de medicamentos genéricos. Ainda que um medicamento genérico pressuponha a existência de um medicamento de referência, os interesses subjacentes às respetivas empresas produtoras de medicamentos de referência são distintos, promovendo inúmeras vezes obstáculos à comercialização de medicamentos genéricos.

Os obstáculos à comercialização de medicamentos genéricos e as necessidades farmacêuticas não satisfeitas na Europa, levaram a Comissão a apresentar uma *Estratégia Farmacêutica para a Europa*, no dia 24 de novembro de 2020, de modo a garantir o acesso dos doentes a medicamentos inovadores e a preços acessíveis, ao mesmo tempo que promove a competitividade, a inovação e a sustentabilidade da indústria farmacêutica europeia. A estratégia possui quatro objetivos principais:

i) Garantir o acesso a medicamentos baratos para os doentes e responder a necessidades médicas (na área da resistência antimicrobiana, do cancro e das doenças raras, por exemplo);

ii) Apoiar a competitividade, a inovação e a sustentabilidade da indústria farmacêutica da UE e o desenvolvimento de medicamentos de elevada qualidade, seguros, eficazes e mais ecológicos;

iii) Melhorar os mecanismos de preparação e resposta a crises;

iv) Garantir uma presença europeia forte no mundo, ao promover um elevado nível das normas de qualidade, eficácia e segurança[265].

[265] COM(2020)761 final.

A *Estratégia Farmacêutica para a Europa* nasce da necessidade de uma nova abordagem europeia que garante um setor farmacêutico forte, equitativo, competitivo e ecológico, que proporcione resultados aos doentes e que explore todo o potencial da transformação digital da saúde e dos cuidados de saúde impulsionada pelos avanços tecnológicos em domínios como a inteligência artificial e a modelização computacional[266].

A Comissão Europeia reconhece o papel da proteção aos produtos e processos inovadores através de direitos de propriedade intelectual, contudo refere que a aplicação desses direitos diverge de Estado-membro para Estado-membro, sobretudo no que se refere às patentes e aos certificados complementares de proteção[267].

Reconhece também, que as indústrias que utilizam a propriedade intelectual de forma intensiva, desempenham um papel essencial na economia da UE e oferecem à sociedade postos de trabalho sustentáveis[268]. Nessa medida, apresenta-se como prioritário a garantia de que os inovadores da UE tenham acesso a instrumentos de proteção rápidos, eficazes e a preços acessíveis, à medida que se elimina a fragmentação provocada pelos diferentes ordenamentos jurídicos. Para que tal aconteça, é necessário garantir o relançamento do *sistema de patente unitária*[269].

Centrando a nossa atenção no domínio do setor farmacêutico europeu, importa recordar que a Comissão está a analisar a forma de continuar a otimizar os incentivos e as recompensas para impulsionar a inovação, de modo a dar resposta a necessidades não satisfeitas, promover a acessibilidade dos preços, assegurar o rápido lançamento no mercado e o fornecimento contínuo de medicamentos, incluindo genéricos e biossimilares[270].

Os objetivos acima vertidos serão brevemente analisados à luz de um novo estudo, que irá ao encontro da perspetiva de Ursula von der Leyen, que aqui reproduzimos:

> "Pessoalmente, não tenho qualquer dúvida: é necessário construir uma união mais forte no domínio da saúde. (…) O futuro será o que nós construirmos. E a Europa será o que nós quisermos que seja. Por isso, deixemos de a menosprezar. E trabalhemos em prol dela. Façamos com que se torne mais forte. E construamos o mundo em que queremos viver. Viva a Europa!" [271]
>
> (Discurso do Estado da União 2020, 16 de novembro)

[266] COM(2020)761 final, p. 1 e 2.
[267] COM(2020) 761 final, p. 11.
[268] COM(2020) 760 final, p. 1.
[269] COM(2020) 760 final, p. 5.
[270] COM(2020) 760 final, p. 6.
[271] Discurso do Estado da União 2020, de Ursula von der Leyen, no dia 16 de novembro de 2020,

8. Conclusões finais

Todo o exposto para concluir que o esboço de um novo panorama certamente passa pelo escrutínio de práticas orientadas por princípios éticos e jurídicos, um alinhamento europeu em defesa dos direitos fundamentais.

Numa altura em que se vive uma situação pandémica, urge uma releitura do catálogo dos direitos humanos e fundamentais já consolidados na maioria dos países ocidentais, de modo a empreender políticas de governação que estejam adaptadas ao atual desenvolvimento de programas e de algoritmos e que sejam concretizáveis quanto à sua aplicabilidade, transparência e auditabilidade, garantindo a proteção multinível da pessoa humana e, com isto, garantir a consolidação dos regimes democráticos, numa perspectiva de cibersegurança.

A Europa está empenhada em fazer avançar os progressos científicos, preservando a liderança tecnológica, desde que as novas tecnologias estejam ao serviço de todos os cidadãos europeus, melhorando as suas vidas e respeitando simultaneamente os seus direitos.

A construção de uma União Europeia para a saúde não é indissociável do espaço europeu de dados de saúde. A saúde, ou mais especificamente, os dados produzidos nessa área são dados eminentemente sensíveis e, portanto, caracterizados como os mais valiosos para a era em que vivemos, a era das novas tecnologias, que se tornaram lugar comum na vidas das pessoas em geral, apesar da subtileza e da permissibilidade.

A proteção de dados de saúde na União Europeia, goza de uma posição preferencial quanto ao sistema protetivo, tornando-se lapidar e modelo para outros países, na medida em que se apresenta como um modelo centrado na dignidade humana. A propósito, a projeção de um elemento ético imprescindível no contorno da atuação da ciência deve, de modo geral, ter uma firmeza a ponto de garantir um bem civilizaconal sem se tornar um obstáculo à inovação. A questão das patentes, nesses termos, ganha destaque em tempos pandémicos em que a sustentabilidade industrial não pode ser paga pelos dados dos pacientes e de demais pessoas que porventura se submetam a ensaios clínicos.

Ao longo da reflexão, vimos que a Comissão Europeia pretende criar uma Agência de investigação e desenvolvimento avançados no domínio biomédico, bem como uma nova Estratégia Farmacêutica Europeia, que analisará a segurança da cadeia de abastecimento da Europa e garantirá o acesso dos cidadãos a medicamentos seguros, a preços acessíveis e de alta qualidade. Central neste novo panorama é a garantia do

lançamento do sistema de patente unitária, um sistema que simplificará a conceção de patentes na União Europeia.

A pandemia da COVID19 provocou um grande ponto de inflexão para a vida humana e, nesse sentido, para a União Europeia, o que implicou a produção de um pensamento em rede, que vai além da busca pelo lucro e do presente nebuloso e, numa perspectiva mais ampla, cria um novo estar no mundo com uma base concreta de sustentabilidade, de coerência, de segurança e de responsabilização.

9. Referências bibliográficas

AGAPITO, Inês. «O Certificado Complementar de Protecção para medicamentos» in Mestrado em Direito de Direito Empresarial Propriedade Industrial e Concorrência Desleal, Universidade Católica, 2015. Disponível em: http://www.evaristomendes.eu/ficheiros/Ines_Agapito-O_Certificado_Complementar_de_Proteccao_de_Medicamentos_(CCP).pdf

ANTUNES, Henrique Sousa. Direito e Inteligência Artificial, Universidade Católica Editora, em parceria com a Fundação Cupertino de Miranda, 2020.

CALDEIRA, Cristina. «O impacto ético e jurídico da aplicação das novas tecnologias na área da saúde» in *Direito da Sociedade do Conhecimento*, Volume I, 2020, p. 222-253. Disponível em: https://bo.europeia.pt/content/files/direito_da_sociedade_do_conhecimento-compactado.pdf

CALDEIRA, C. e SARLET, G. «O consentimento informado e a proteção de dados pessoais de saúde na Internet – uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana» in *Direito da Sociedade do Conhecimento*, 2020, p. 256-280. Disponível em: https://bo.europeia.pt/content/files/direito_da_sociedade_do_conhecimento-compactado.pdf

CALDEIRA, Cristina e FERNANDES, Márcia. «A partilha de dados pessoais sensíveis, dados epidemiológicos (COVID-19) e genéticos: aspectos jurídicos e bioéticos na perspetiva da União Europeia, Portugal e Brasil» in *Direito da Sociedade do Conhecimento*, 2020, p. 322-375. Disponível em: https://bo.europeia.pt/content/files/direito_da_sociedade_do_conhecimento-compactado.pdf

CAMPOS, António Correia de. Comentário ao artigo nº 168.º TFUE, in *Tratado de Lisboa, anotado e comentado*, Manuel Lopes Porto e Gonçalo Anastácio (Coord.), Editora Almedina, Coimbra, 2012.

CARNEIRO, António, V. «Inteligência Artificial em Saúde e os seus problemas», Revista Visão, 25 de agosto de 2018. Disponível em: https://visao.sapo.pt/opiniao/bolsa-de-especialistas/2018-08-25-inteligencia-artificial-em-saude-e-os-seus-problemas/

COECKELBERGH, Mark. *AI ETHICS,* The MIT Press Essential Knowledge series, London, 2020.

COMISSÃO EUROPEIA

____ Discurso da Presidente da Comissão Europeia no evento de apresentação do "Masters of Digital 2021", Bruxelas, dia 4 de fevereiro de 2021. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_419

____Proposta de Regulamento do Parlamento Europeu e do Conselho sobre um Mercado Único de Serviços Digitais «Lei dos Serviços Digitais» e que altera a Diretiva 2000/31 / CE COM(2020)825 final, 2020/0361(COD), Bruxelas, 15 de dezembro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/pt/ALL/?uri=COM:2020:825:FIN.

____Programa Europa Digital, Bruxelas, 14.12.2020. Disponível em: https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme.

____Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector «Digital Markets Act», COM(2020)842 final, 2020/0374 (COD). Bruxelas, 15 de dezembro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=pt

____ Comunicação da Comissão do Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, «Estratégia Farmacêutica para a Europa», COM(2020) 761 final, Bruxelas, 25 de novembro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0761&from=EN

____ Comunicação da Comissão do Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, «Tirar pleno partido do potencial de inovação da UE Um plano de ação em matéria de propriedade intelectual para apoiar a recuperação e resiliência da UE», COM(2020) 760 final, Bruxelas, 25 de novembro de 2020. Disponível em: https://ec.europa.eu/transparency/regdoc/rep/1/2020/PT/COM-2020-760-F1-PT-MAIN-PART-1.PDF

____Comunicação «Programa de Trabalho da Comissão 2021, Uma União vital num mundo fragilizado», COM (2020)690 final, Bruxelas, 19.10.2020. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:91ce5c0f-12b6-11eb-9a54-01aa75ed71a1.0006.02/DOC_1&format=PDF

____Preparação para as estratégias de vacinação contra a COVID-19 e a disponibilização das vacinas, COM (2020)680 final, Bruxelas, 15 de outubro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020DC0680

____Plano de Ação para a Educação Digital (2021-2027), «Reconfigurar a educação e a formação para a era digital», COM (2020)624 final, Bruxelas, 30 de setembro de 2020. Disponível em: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_pt

____Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho e ao Banco Europeu de Investimento, «Estratégia da UE para as vacinas contra a COVID-19», COM (2020)245 final, Bruxelas, 17 de junho de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0245&from=EN

____Proposta de regulamento do Parlamento Europeu e do Conselho de criação de um programa de ação da União no domínio da saúde para o período 2021-2027 e que revoga o Regulamento (UE) n.º 282/2014 «Programa UE pela Saúde», COM/2020/405 final, 28 de maio de 2020, p. 8. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9b76a771-a0c4-11ea-9d2d-01aa75ed71a1.0023.02/DOC_1&format=PDF

____Comunicação da Comissão do Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, «Uma nova estratégia industrial para a Europa», COM (2020)102 final, Bruxelas, 10 de março de 2020.

___ Comunicação da Comissão do Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, «Construir o futuro digital da Europa», COM (2020)67 final, Bruxelas, 19 de fevereiro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0067&from=EN

____A European strategy for data, COM(2020)66 final, Bruxelas, 19 de fevereiro de 2020. Disponível em: https://ec.europa.eu/info/sites/info/files/communication-europeanstrategy-data-19feb2020_en.pdf

____ Livro Branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança, COM (2020)65 final, Bruxelas, 19 de fevereiro de 2020. Disponível em: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf

____ Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica, COM (2020)64final, Bruxelas, 19 de fevereiro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0064&from=en
____ Comunicação sobre «As regras de proteção de dados como instrumento gerador de confiança dentro e fora da UE – ponto da situação», COM(2019)374 final, Bruxelas, 24 de julho de 2019. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:52019DC0374&from=EN
____ Comunicação sobre «Aumentar a confiança numa inteligência artificial centrada no ser humano» COM(2019)168 final, Bruxelas, 8 de abril de 2019. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019DC0168&from=EN
____Comunicação sobre «Plano Coordenado para a Inteligência Artificial», COM(2018)795 final, 251 Bruxelas, 7 e dezembro de 2018. Disponível em: https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-795-F1-PT-MAIN-PART-1.PDF
___ Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial. *Orientações éticas para uma inteligência artificial*, junho 2018. Disponível em: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence
___ Comunicação da Comissão do Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, «Inteligência artificial para a Europa», COM (2018)237 final, Bruxelas, 25 de abril de 2018. Disponível em: https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-237-F1-PT-MAIN-PART-1.PDF
____Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), Bruxelas, COM (2017) 10 final, de 10 de janeiro de 2017. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

CULLET, Philippe. «Patents and medicines: the relationship between TRIPS and the human right to health» in International Affairs 79, I (2003), 139-160. Disponível em: https://library.fes.de/libalt/journals/swetsfulltext/17639153.pdf

INPI- INSTITUTO NACIONAL DE PROPRIEDADE INDUSTRIAL. «Importância das patentes na área da saúde (medicamentos e vacinas)», abril de 2020. Disponível em: https://inpi.justica.gov.pt/Portals/6/PDF%20INPI/Not%C3%ADcias%20-%20ficheiros%20de%20apoio/Import%C3%A2ncia%20das%20patentes%20na%20%C3%A1rea%20da%20sa%C3%BAde%20(medicamentos%20e%20vacinas).pdf?ver=2020-04-26-122645-213

JOUE - JORNAL OFICIAL DA UNIÃO EUROPEIA
____Carta dos Direitos Fundamentais da União Europeia. (JOUE nº C-364/1). Bruxelas, 10.12.2000. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf.
____ Diretiva (UE) 2016/680, de 27.04.2016. 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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT
____ Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9.03.2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88), Bruxelas, de 4.4.2011 252.
____Recomendação (UE) 2020/518, da Comissão, de 8 de abril de 2020, relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para

combater a crise da COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados, Bruxelas, 14.04.2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32020H0518&from=PT

____ Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Resolução do Conselho de Ministros n.º 41/2018 publicada em Diário da República, 1.ª série — N.º 62 — 28 de março de 2018. http://www.sg.pcm.gov.pt/media/33586/02.pdf. Ratificação 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 L 119), Bruxelas, 4.5.2016. Disponível em: http://www.sg.pcm.gov.pt/media/33583/01pdf_dados.pdf

____Regulamento (UE) 2019/933 do Parlamento Europeu e do Conselho de 20 de maio de 2019 que altera o Regulamento (CE) n.o 469/2009 relativo ao certificado complementar de proteção para os medicamentos (L 153/1), Bruxelas, 11 de junho de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0933&from=EN

____Tratado da União Europeia (Versão Consolidada), C-326/13, Bruxelas, 26.10.2012. Disponível em:
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:0013:0046:PT:P DF.

MACHADO, João Baptista. *Lições de Direito Internacional Privado*, 3ª Edição atualizada (reimpressão), Almedina, Coimbra, 2017, p. 386-392.

MARQUES, Remédio. Comentário ao artigo nº 118.º TFUE in *Tratado de Lisboa*, Manuel Lopes Porto e Gonçalo Anastácio (Coord.), Almedina, Coimbra, 2012.

MARTINO, A. Anselmo. «Logic, Informatics, Artificial Intelligence And Technology In Law: History And Challenges» in *Law, Tecnologhy and Innovation*, *V.II. Insights on Atificial Intelligence and the Law*, Expert Editora Digital, Leonardo Parentoni e Renato César Cardoso (Org.), 2020, p.28-48.

MASSENO, Manuel D. «Das Consequências Jurídicas da Adesão do Brasil aos Princípios da OCDE para a Inteligência Artificial, Especialmente em Matéria de Proteção de Dados», Revista Campo Jurídico, Revista Campo Jurídico, barreiras-BA v.8 n.1, p.113-122 julho-dezembro, 2020.

OMS-ORGANIZAÇÃO MUNDIAL DA SAÚDE «Public Health, Innovation and Intellectual Property Rights», 2006, p.19, 20 e 21. Disponível em:
https://www.who.int/intellectualproperty/documents/thereport/ENPublicHealthReport.pdf?ua=1

OCDE-ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO. «Recomendação do Conselho da Inteligência Artificial», aprovada em 22 de maio de 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

PARLAMENTO EUROPEU

____Relatório sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial (2020/2015(INI), 2 de outubro 2020. Disponível em: https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_PT.html

____Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas, P9TA(2020)0275. Disponível em:
https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html

____Resolução de 16.02.2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL). Disponível em:
https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html#title1

VICENTE, Dário Moura. «Inteligência Artificial e Iniciativas Internacionais», in *Inteligência Artificial & Direito,* Coordenação Manuel Lopes Rocha e Rui Soares Pereira; editora Almedina, Coimbra, 2020, p.93-105.
____Fichas temáticas sobre a União Europeia, 2021. Disponível em: www.europarl.europa.eu/factsheets/pt

PINHEIRO, Luís de Lima. *Direito Internacional Privado, Volume II – Direito de Conflitos – Parte Especial*, 4ª edição refundada, Almedina, Coimbra, 2018, p. 630.

PRESIDÊNCIA PORTUGUESA DO CONSELHO DA UNIÃO EUROPEIA. "The Intelellectual Property metamorphosis in the Age of Digital Transition", de 11 de fevereiro de 2021. Disponível em: https://www.2021portugal.eu/pt/noticias/a-metamorfose-da-propriedade-intelectual-na-era-da-transicao-digital/

SILVA, Pedro Sousa e. *Direito Industrial*, 2ª edição, Editora Almedina, Coimbra, 2020.

SNS-SERVIÇO NACIONAL DE SAÙDE.
Plano de Vacinação COVID-19, 3 de dezembro de 2020. Disponível em:
https://www.sns.gov.pt/wp-content/uploads/2019/06/PlanoVacinacaoCovid_19.pdf

WIPO/OMPI-WORLD INTELLECTUAL PROPERTY ORGANIZATION. Perguntas e Respostas sobre o PCT. Disponível em:
https://www.wipo.int/export/sites/www/pct/pt/basic facts/faqs about the_pct.pdf

____ASSEMBLIES OF THE MEMBER STATES OF WIPO Thirty-Sixth Series of Meetings Geneva, September 24 to October 3, 2001, A/36/14, 6 de agosto de 2001, p. 4.
Disponível em: https://www.wipo.int/edocs/mdocs/govbody/en/a_36/a_36_14.pdf

Legislação

Constituição da República Portuguesa, de 1976.
Decreto-Lei n.º 176/2006, de 30 de agosto, atualizado pelo Decreto-Lei n.º 112/2019, de 16 de agosto, estabelece o regime jurídico dos medicamentos de uso humano, transpondo a Diretiva n.º 2001/83/CE do Parlamento Europeu e do Conselho, de 6 de novembro de 2006.
Decreto-Lei nº 110/2018, de 10 de dezembro, que a prova o novo Código da Propriedade Intelectual, transpondo as Diretivas (UE)2015/2436 e (UE) 2016/943.
Lei n.º 26/2016, de 28 de agosto atualizada pela Lei nº 33/2020, de 12 de agosto, Informação administrativa nominativa
Lei n.º 12/2005, de 26 de janeiro, Informação genética pessoal e informação de saúde, atualizada pela Lei n.º 26/2016, de 28 de agosto

Teletrabalho – a Nova Normalidade?

João Massano[394]

RESUMO

A Origem remonta à década de 70 do século XX, massificou-se com situação pandémica.
Ao teletrabalho, têm sido apontadas vantagens, por gerar empregabilidade, e desvantagens por dificultar o trabalho "em rede".
Em Portugal, a figura do teletrabalho (subordinado) foi introduzida no C.T. de 2003 (arts. 233.º a 243.º), definido no art. 165.º do Código do Trabalho de 2009. Prevê duas modalidades: Externo – Celebrado contrato com trabalhador que não pertence à Empresa (art. 166.º, n.º 1, do CT); Interno – Trabalhador da Empresa passa a desempenhar funções neste regime (art. 166.º, n.º 1, do CT);
Na situação Jurídica do Teletrabalhador importa chamar à colação o princípio da igualdade de tratamento do teletrabalhador em relação aos restantes trabalhadores, prevendo os mesmos direitos e deveres, como, por exemplo, o respeito pela privacidade do teletrabalhador, limitando as visitas ao domicílio ao período das 09 - 19 horas (em dia normal de trabalho) e a obrigação de estar contactável durante o seu horário.
No que concerne ao Regime Excecional do Teletrabalho durante a Pandemia, entre as primeiras medidas legislativas para prevenção adotadas pelo Governo através do DL n.º 10-A/2020, de 13 de Março, houve a possibilidade de aplicarem o Teletrabalho. Actualmente, será obrigatório, independente do pedido do trabalhador, desde que compatível com as suas funções.

PALAVRAS-CHAVE

Teletrabalho; Pandemia; Teletrabalhadores; Direitos; Deveres.

[394] Presidente do Conselho Regional de Lisboa da Ordem dos Advogados

Remote Working – The New Standard?

ABSTRACT

It’s origin dates back to the 70's of the 20th century, becoming popular with the pandemic situation.
Advantages to remote working have been pointed out like jobs creation and disadvantages like making networking harder.
In Portugal, the figure of remote working was introduced in the C.T. of 2003 (arts. 233 to 243), defined in art. 165 of the 2009 Labor Code. It establishes two modalities:
a) External - A contract was signed with a worker who does not belong to the Company (art. 166, no. 1, CT);
b) Internal - Company employee takes up his duties under this regime (art. 166, no. 1, CT);
In the Legal situation of the remote worker, it is important to talk about the equal treatment principle of the remote worker in relation to other workers, assuring the same rights and duties, ie: respect for the privacy of the remote worker, limiting home visits to the period from 9 am to 7 pm (on a working day) and the obligation to be reachable during working hours.
With regard to the Exceptional Remote Work Scheme during the Pandemic, among the first legislative measures for prevention adopted by the Government through DL n.º 10-A / 2020, March 13th, there was the possibility of applying remote working. Currently, it is mandatory, regardless of the employee's request, as long as it is compatible with their duties.

KEYWORDS

Remote working; Pandemic; Remote workers; Rights; Duties.

1. Origem do fenómeno

Desenvolvimento da sociedade de informação a partir da década de 70 do século XX, resultante dos avanços tecnológicos nas áreas da informática e telecomunicações.

Apesar da difusão do teletrabalho nos setores dos serviços mais informatizados (v.g. na banca e seguros), o fenómeno não se massificou até à recente situação pandémica. Nota: estatísticas apontavam para cerca de 8% dos contratos de trabalho na Europa e apenas 3% em Portugal serem executados em regime de teletrabalho [395].

2. Vantagens e inconvenientes

Por um lado, o teletrabalho potencia empregabilidade não só de pessoas com dificuldades de locomoção, mas da generalidade dos trabalhadores nesta era da globalização (sobretudo no setor terciário), que poderão desempenhar funções para empresas situadas em regiões e países distantes da sua área de residência; permite aos trabalhadores reduzir despesas e evitar o tempo das deslocações entre a residência e as instalações da entidade empregadora; permite às empresas reduzir os custos fixos com postos de trabalho, possibilitando terem instalações com menores dimensões (fomentando o outsourcing); além disso, terá vantagens ambientais, como redução da poluição atmosférica (em virtude da menor necessidade de circulação em meios de transportes públicos e privados).

Por outro lado, tem sido apontado que o teletrabalho dificulta o trabalho "em rede" (colaboração instantânea entre colegas presentes no mesmo local), bem como o controlo das condições de trabalho pela entidade empregadora, potenciando o isolamento do trabalhador e o desgaste psicológico inerente, além de haver um risco acrescido de invasão da sua esfera privada (especialmente se o teletrabalho for prestado a partir da residência) e maior vulnerabilidade dos dados pessoais e da empresa partilhados.

Contudo, alguns dos inconvenientes apontados podem atualmente ser minimizados através dos meios tecnológicos disponíveis, mediante realização de videoconferências e videochamadas com múltiplos intervenientes, facilitando a partilha entre colegas, existindo até programas informáticos que permitem um controlo sofisticado por parte das empresas da atividade desenvolvida pelos seus trabalhadores [396].

---

[395] Esta percentagem, segundo o EUROFUND, data de 2007, e engloba trabalho subordinado e não subordinado. Em 2017 o EUROFUND coloca Portugal ainda na cauda da Europa, mas com uma percentagem de 11% dos profissionais (subordinados e não subordinados) em trabalho remoto, e destes, só 2% a título permanente.

[396] Por exemplo: programas Basecamp (gestão de projetos); Whereby e Skype (partilhas de ecrã, demonstração de produtos, videoconferências); Dropbox (centralização de ficheiros); Google Docs (colaboração na elaboração de documentos).

Sendo controverso se o teletrabalho aumenta ou reduz a produtividade, bem como se potencia ou diminui a conciliação entre a vida profissional e pessoal dos trabalhadores, tal dependerá das circunstâncias em que o teletrabalhador(a) desempenha as suas tarefas.
Nota: tem vindo a ser discutida a consagração geral do direito à desconexão do trabalhor (o Governo apresentou uma proposta de lei na Assembleia da República), salientando-se as dificuldades de prestação de teletrabalho de trabalhadores com filhos, em caso de suspensão das atividades letivas presenciais nas escolas (como sucedeu recentemente durante o estado de emergência e continuou para diversos graus de ensino durante o estado de calamidade que se seguiu).

3. Tipos de teletrabalho.

Consoante o local de desenvolvimento da atividade do trabalhador, o teletratrabalho poderá ser prestado a partir do domicílio (modalidade mais vulgarizada) ou em instalações criadas especificamente para o efeito (denominadas *telecottagges*), partilhadas por trabalhadores da mesma empresa ou de diferentes empresas.
Nota: não confundir com o trabalho prestado em "*escritório-satélite*", que não deixam de ser instalações da empresa, mas com caráter secundário.

Consoante o grau de intensidade da comunicação infomática ou telemática entre trabalhador e entidade empregadora, o teletrabalho pode ser prestado de forma permanente, intermitente ou esporádica (*on line*, *off line* ou mista).

Consonante o grau de autonomia do teletrabalhador, o teletrabalho poderá constituir:

a) trabalho subordinado, com base em contrato de trabalho sujeito a regime especial (previsto no art. 165.º a 171.º do Código do Trabalho);
b) trabalho autónomo, com base em contrato de prestação de serviços, a que será aplicável subsidiariamente o regime do contrato de mandato ou empreitada (previsto no Código Civil);
c) trabalho autónomo, mas com dependência económica, enquadrado no regime do trabalho no domícilio (previsto na Lei n.º 101/2009, de 8 de Setembro).

4. Noção legal e modalidades de teletrabalho

Em Portugal, a figura do teletrabalho (subordinado) foi introduzida no Código de Trabalho de 2003 (arts. 233.º a 243.º), estando atualmente definido no art. 165.º do Código do Trabalho de 2009, com duas notas características:

a) a natureza da atividade laboral envolver essencialmente o recurso a tecnologias de informação e de comunicação

   - os dois elementos são cumulativos e não simples instrumentos de trabalho (ex: advogado da empresa que elabore em casa um documento jurídico em computador e o envie por correio eletrónico, não se torna só por isso um teletrabalhador);

b) a distância do local de trabalho relativamente às instalações da entidade empregadora

   - o trabalho deve ser realizado habitualmente fora das instalações da empresa, mas não necessariamente no domicílio do trabalhador, sendo que este poderá deslocar-se esporadicamente àquelas instalações para prestar alguma atividade, sem que tal descaracterize o teletrabalho.

O Código do Trabalho prevê duas modalidades do teletrabalho:

a) *externo* – quando é celebrado um contrato de teletrabalho com um trabalhador que não pertença à empresa (art. 166.º, n.º 1, do CT);

   - o contrato de teletrabalho está sujeito a forma escrita e tem de conter uma série de elementos (art. 166.º, n.º 4), podendo ser modificado para um contrato de trabalho comum, por determinado período ou a título definitivo (art. 166.º, n.º 5)

   Nota: o contrato de teletrabalho pode ser celebrado a termo, desde que haja fundamento legal (vd. arts. 139.º e segs do CT)[397]

b) *interno* – quando um trabalhador da empresa passa a desempenhar funções em regime de teletrabalho, mediante acordo com a entidade empregadora (art. 166.º, n.º 1, do CT);

   - o acordo de teletrabalho está sujeito a um prazo inicial máximo de 3 anos, salvo se outro for o prazo estabelecido em IRCT aplicável (art. 167.º. n.º 1, do CT), tendo ambas as partes um direito ao arrependimento, podendo fazer cessar o acordo de teletrabalho nos primeiros 30 dias da sua execução (art. 167.º, n.º 2), retomando o trabalhador a forma inicial de prestação da sua atividade (art. 167.º, n.º 3)

A forma escrita para o contrato/acordo de teletrabalho não é requisito para a sua validade, mas apenas para a prova da sua celebração (cf. art. 166.º, n.º7, do CT).

O Código do Trabalho prevê duas situações excecionais em que a passagem para o regime de teletrabalho é um direito do trabalhador da empresa, não dependente do acordo da entidade empregadora, que não poderá recusar a pretensão do trabalhador (cf. art. 166.º, n.,º 4, do CT):

1) trabalhador vítima de violência doméstica (art. 166.º, n.º 2 do CT)

[397] Nesta parte da exposição estás a utilizar uma versão anterior a 2015, sem o aditamento do novo n.º 3 da versão em vigor, pela L 120/2015, de 01/09).

- requisitos : trabalhador ter apresentado queixa-crime e se ter ausentado da casa de morada de família (vd. art. 195.º, n.º 1 do CT), e a natureza da respetiva atividade laboral ser compatível com o teletrabalho

- caberá ao empregador avaliar tecnicamente se as funções do trabalhador poderão ser desempenhadas fora das instalações da empresa, com recurso intensivo às tecnologias de informação e de comunicação

2) trabalhador com filho menor de 3 anos (art. 166.º, n.º 3, do CT)

- requisitos: a natureza da atividade laboral ser compatível com o teletrabalho e "*a entidade patronal disponha de recursos e meios para o efeito*"

- medida que visa promover a conciliação da vida profissional, mas aquela cláusula aberta e vaga poderá permitir à entidade empregadora inviabilizar o exercício do direito do trabalhador a prestar serviço em regime de teletrabalho, na medida em que será dificil sindicar a falta de "*recursos*" ou "*meios*" (no limite, o empregador poderia recusar o pedido do trabalhador a pretexto de não poder dispensar um computador para colocar em casa do trabalhador ou não poder prescindir da sua presença nas instalações da empresa).

5. A Situação jurídica do teletrabalhador

O princípio essencial é da igualdade de tratamento do teletrabalhador em relação aos restantes colegas de trabalho, "*nomeadamente no que se refere a formação e promoção ou carreira profissionais, limites do período normal de trabalho e outras condições de trabalho, segurança e saúde no trabalho e reparação de danos emergentes de acidente de trabalho ou doença profissional"* (art. 169.º, n.º 1, do CT), devendo ser promovidos os contactos com a empresa e demais trabalhadores, a fim de evitar o isolamento do teletrabalhador (art. 169.º, n.º 3, do CT).

Assim, no regime de teletrabalho, o trabalhador terá os mesmos direitos e deveres dos demais trabalhadores da empresa, designadamente, direito a receber a retribuição integral – incluindo subsídio de refeição [398](salvo se no contrato de trabalho ou em IRCT aplicável se estipular que o pagamento de tal subsídio está dependente do trabalhador desempenhar as suas funções nas instalações da empresa), estando obrigado a prestar serviço durante o período normal de trabalho, no horário estabelecido pela entidade empregadora.

Quanto aos instrumentos de trabalho respeitantes às tecnologias de informação e comunicação, é estabelecida uma presunção de que serão propriedade do empregador,

[398] Matéria controversa, ainda que o atual art.º 5.º do Decreto 3-A/21 determine o seu pagamento.

que deverá assegurar a sua instalação, manutenção e pagamento das despesas inerentes, sem prejuízo do dever de custódia do trabalhador relativamente àqueles elementos (art. 168.º, n.º 1 do CT)

Tal presunção, poderá ser afastada no contrato/acordo de teletrabalho, se nele ficar estipulado que os meios utilizados são pertencentes ao teletrabalhador, embora seja controverso que a entidade empregadora possa exigir ao teletrabalhador que suporte encargos adicionais com aquisição de computador e serviço de acesso à internet.

Relativamente ao controlo da atividade do teletrabalhador pela entidade empregadora, bem como da utilização dos instrumentos de trabalho que sejam propriedade da empresa, o legislador preocupou-se com respeito pela privacidade do teletrabalhador, limitando as visitas ao domicílio ao período das 09 às 19 horas (em dia normal de trabalho), de modo a assegurar os tempos de descanso do trabalhador e de repouso da sua família (art. 170.º, n.º 1 e 2 do CT).

Além disso, a entidade empregadora poderá impor que o teletrabalhador esteja contactável por email, telefone, videochamada, durante o horário de trabalho, mas não poderá impor que o trabalhador tenha permanentemente uma câmara de vídeo ligada durante o período de trabalho, nem outros sistemas de videovigilância, atendendo à proibição geral de utilização de meios de vigilância à distância (cf. art. 20.º, n.º 1, do CT), salvo casos excecionais e sujeitos a autorização prévia da CNPD (cf. arts. 20.º, n.º 2 e 21.º, n.º 1, CT).

Recentemente, perante a massificação da utilização do teletrabalho no período de confinamento da população em casa, para evitar/mitigar o contágio pelo novo coronavírus, a Comissão Nacional de Proteção de Dados emitiu, no passado dia 17 de Abril, um documento com orientações no sentido de não serem legalmente admissíveis, por implicarem um controlo desproporcional (vd. art. 21.º, n.º 2, do CT) - superior ao normalmente existente quando o trabalhador tem local de trabalho na empresa - «*softwares que, para além do rastreamento do tempo de trabalho e de inatividade, registam as páginas de Internet visitadas, a localização do terminal em tempo real, as utilizações dos dispositivos periféricos (ratos e teclados), fazem captura de imagem do ambiente de trabalho, observam e registam quando se inicia o acesso a uma aplicação, controlam o documento em que se está a trabalhar e registam o respetivo tempo gasto*

em cada tarefa (v.g., TimeDoctor, Hubstaff, Timing, ManicTime, TimeCamp, Toggl, Harvest)» [399].

Portanto, segundo a CNPD, a forma de controlo da prestação do teletrabalhador terá de passar pela definição de tarefas e prazos (razoáveis) para o seu cumprimento, sujeito a reportes periódicos, bem como determinação de contatos periódicos com empresa, por email e telefone, realização de teleconferências, excluindo meios de controlo informático que põe em causa a privacidade dos trabalhadores.

6. Evolução do regime excecional do teletrabalho durante a pandemia Covid19

Entre as primeiras medidas legislativas para prevenção, contenção, mitigação da infeção epidemiológica decorrentes do novo coronavírus e doença Covid-19, adotadas pelo Governo através do **Decreto-Lei n.º 10-A/2020**, de 13 de Março, destacou-se a possibilidade de qualquer das partes, trabalhador ou empregador, determinar unilateralmente a aplicação temporária do regime de teletrabalho (subordinado) – portanto, **sem necessidade de acordo** (como é a regra geral no Código de Trabalho) – "*desde que compatível com as funções exercidas"* (cf. art. 29.º, n.º 1 do DL 10-A/2020).

Portanto, o único requisito da aplicação do regime excecional de prestação de teletrabalho era compatibilidade das funções do trabalhador com o desempenho fora das instalações da entidade empregadora, através do recurso às tecnologias de informação e comunicação (cf. art. 165.º do CT).

Não sendo conhecida jurisprudência sobre a matéria, a doutrina considera que a entidade empregadora terá bastante "latitude" na apreciação da compatibilidade do teletrabalho com a atividade dos trabalhadores ao seu serviço, face ao poder de conformação da mesma pelo empregador (art.º 115.º do CT), importando atender à categoria profissional de cada trabalhador (vd. arts. 118.º e 120.º do CT).

Contudo, foi excluída a aplicação de tal regime excecional de prestação de teletrabalho aos trabalhadores de serviços essenciais (v.g. profissionais de saúde, das forças e serviços de segurança e de socorro, incluindo os bombeiros voluntários, e das forças armadas) – cf. art.º 29.º, n.º 2 e 10.º do DL 10-A/2020.

A vigência de tal regime excecional, de prestação de teletrabalho independente de acordo (para a generalidade dos trabalhadores, e não apenas nas duas situações previstas

[399] Este aspeto de natureza tecnológica é importante desenvolver.

no Código do Trabalho), só cessou com a sua revogação pelo Decreto-Lei n.º 24-A/2020, de 29 de Maio (vd. art. 4.º).

No entanto, **durante todo o período de estado de emergência**, declarado e renovado pelo Presidente da República, entre os dias 19 de Março e 1 de Maio (cf. Decretos do PR n.º 14-A/2020, de 18/03, n.º 17-A/2020, de 02/04, e n.º 20-A/2020, de 17/04), o Governo, no âmbito do seu poder de regulamentação do estado de emergência, tornou "***obrigatória a adoção do regime de teletrabalho**, independentemente do vínculo laboral, sempre que as funções em causa o permitam*" (cf. art. 8.º dos Decretos do Governo n.º 2-A/2020, de 20/03, n.º 2-B/2020 de 02/04, e n.º 2-C/2020, de 17/04).

Apesar da redação distinta, o único requisito para a obrigatoriedade da aplicação do regime do teletrabalho era essencialmente idêntico ao estabelecido no DL 10-A/2020: a possibilidade das funções do trabalhador serem desempenhadas fora das instalações da empresa, com recurso intensivo às tecnologias de informação e de comunicação.

Tal obrigatoriedade de adoção do teletrabalho visou potenciar o cumprimento do dever geral de recolhimento domiciliário estabelecido durante o estado de emergência, embora não tenham deixado de ser permitidas as deslocações dos cidadãos para desempenho de atividades profissionais, quando não fosse viável desempenharem funções em teletrabalho (cf. art. 5.º, n.º 1, alínea b), dos Decretos do Governo n.º 2-A/2020, de 20/03, n.º 2-B/2020 de 02/04, e n.º 2-C/2020, de 17/04).

Com a passagem ao regime de calamidade pública, foi mantida a obrigatoriedade da prestação de teletrabalho (cf. art. 4.º do regime anexo à Resolução do Conselho de Ministros n.º 33-A/2020, de 30 de Abril), sendo que, a partir de 18 de Maio, passou a estabelecer-se que, no caso de não ser possível o teletrabalho, as entidades empregadoras deveriam organizar "*escalas de rotatividade de trabalhadores, diárias ou semanais, e com horários diferenciados de entrada e saída"* (cf. art. 4.º, n.º 2, do regime anexo à Resolução do Conselho de Ministros n.º 38/2020, de 17 de Maio).

Na sequência da revogação do regime excecional da prestação de teletrabalho que estava previsto no art. 29.º do DL 10-A/2020 (pelo DL 24-A/2020), em 29 de Maio, o Governo eliminou a obrigatoriedade de adoção do teletrabalho para generalidade dos trabalhadores, passando apenas a referir (recomendar ?) a sua adoção pelas entidades empregadoras, com vista a prevenir de riscos de contágio decorrentes da pandemia da doença Covid-19 (cf. art. 4.º, n.º 1, da Resolução do Conselho de Ministros n.º 40-A/2020, de 29 de Maio).

Destarte, **voltou a aplicar-se o regime de teletrabalho previsto no Código do Trabalho,** portanto, dependente do acordo entre empregador e trabalhador, mas prevendo-se mais três situações excecionais em que o trabalhador pode impor unilateralmente a aplicação temporária do regime de teletrabalho (cf. art. 4.º, n.ºs 2 e 3 da RCM n.º 40-A/2020):

a) trabalhadores que sejam doentes de maior risco em caso de infeção pelo coronavirus (imunodeprimidos e outros doentes crónicos, indicados no art. 25.º-A do DL 10-A/2020);
b) trabalhadores com grave deficiência (grau de incapacidade igual ou superior a 60%);
c) trabalhadores que tenham a seu cargo filhos menores de 12 anos (ou com deficiência ou doença crónica), em virtude da suspensão decretada das atividades em creches, jardins de infância letivas (aplicável apenas a um dos progenitores, independentemente do número de filhos …).

Além disso, **o regime do teletrabalho só é obrigatório**, desde que "*as funções em causa o permitam*"**, no caso e na medida em que a entidade empregadora não consiga assegurar o cumprimento das orientações da DGS e ACT nas suas instalações, por tal não ser viável nos espaços físicos que dispõe e face à organização do trabalho** (cf. art. 4.º, n.º 4 da RCM n.º 40-A/2020)**.**

No caso de não ser adotado o teletrabalho, recomendou-se o estabelecimento de "*escalas de rotatividade de trabalhadores entre o regime de teletrabalho e o trabalho prestado no local de trabalho habitual, diárias ou semanais, horários diferenciados de entrada e saída, horários diferenciados de pausas e de refeições*" (cf. art. 4.º, n.º 5 da RCM n.º 40-A/2020).

Com o termo do ano letivo e a reabertura das creches e jardins de infância, veio a ser eliminada a obrigatoriedade de aplicação do teletrabalho a requerimento de trabalhador com filhos entre os 3 e os 12 anos a cargo, a partir do dia 1 de Julho (cf. art. 4.º do regime anexo à Resolução do Conselho de Ministros n.º 51-A/2020, de 26 de Junho).

Atualmente rege o art. 5.º, do Decreto 3-A/21, de 14/01, por efeito do 3-D/21, de 29/01, até 14 de fevereiro de 2021, **mantendo-se as situações excecionais de prestação obrigatória de teletrabalho a requerimento do trabalhador**, desde que compatível com as suas funções:

a) trabalhador vítima de violência doméstica (verificando-se os requisitos do art. 195.º, n.º 1, do CT – apresentada queixa-crime e ausência da casa de morada de família);
b) trabalhador com menor de 3 anos a cargo (verificando o requisito do art. 166.º, n.º 3, do CT – a enitidade empregadora dispor de "recursos e meios" para o teletrabalho);
c) trabalhador imunodeprimido ou portador de doença crónica que seja considerado doente de risco (designadamente, os hipertensos, os diabéticos, os doentes cardiovasculares, os portadores de doença respiratória crónica, os doentes oncológicos e os portadores de insuficiência renal – cf. art. 25º-A do DL 10-A/2020)
d) trabalhadores com grave deficiência (grau de incapacidade igual ou superior a 60%).

Acresce que **o teletrabalho será obrigatório**, independente do pedido do trabalhador, desde que compatível com as suas funções, **caso não seja possível cumprir as orientações da DGS e ACT**, relativas à prevenção dos riscos de contágio, decorrentes da pandemia da doença Covid-19, nas instalações da empresa.

Nota: quanto à situação jurídica do teletrabalhador, nenhum dos regimes excecionais de teletrabalho estabelecidos, quer durante o atual[400] estado de emergência, que durante os estados de estado de calamidade/contingência/alerta que o antecederam (consoante a região do país), alterou os direitos e deveres e demais condições de trabalho aplicáveis [acima sumariadas no ponto 5].

[400] Atualmente estamos, novamente, em emergência: Decreto do Presidente da República n.º 9-A/2021, Resolução da Assembleia da República N.º 14-A/2021 - Diário da república N.º 19/2021, 1.º suplemento, série i de 2021-01-28 e Decreto n.º 3-D/2021 - Diário da República n.º 20/2021, 1.º suplemento, série I de 2021-01-29, que regulamenta o estado de emergência decretado pelo Presidente da República.

Nas Fronteiras da Propriedade Intelectual: os direitos patrimoniais sobre dados, uma perspetiva europeia[401]

Manuel David Masseno[402]

RESUMO

Com a relevância económica crescente dos megadados, sobretudo por força da *Internet das Coisas* e da Inteligência Artificial, a dicotomia entre a informação livre e a apropriável em exclusivo por ser o resultado da atividade humana estruturada criativamente, a Propriedade Intelectual, já não basta. Consequentemente e desde os últimos anos do Século XX, a União Europeia tem procurado novas abordagens para além da PI, como as relativas à regulação das bases de dados não criativas ou o *saber-fazer* e os segredos de negócios, estando em debate a atribuição de direitos aos "criadores de dados não-pessoais", pelo menos através da autorregulação, enquanto são procuradas alternativas.

PALAVRAS-CHAVE

Autorregulação; dados não pessoais; Propriedade Intelectual; União Europeia.

ABSTRACT

Along with the increased economic importance of big data, mostly in consequence of IoT and Artificial Intelligence, the dichotomy between free and owned information as a result of human creative work, Intellectual Property, is no longer enough. Hence and since the final years of the XX Century, the European Union has pursued new approaches beyond IP, as those regarding the regulation of non-creative databases or of know-how and trade secrets, being the current debate on issuing rights to "originators" of non-personal data, at least through self-regulation, meanwhile alternatives are searched.

KEYWORDS

European Union; Intellectual Property; non-personal data; Self-regulation.

---

[401] Este texto corresponde à Conferência realizada no *CODAIP 2020 – XIV Congresso de Direito de Autor e Interesse Público*, organizado pelo GEDAI – Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná, em Curitiba, Brasil, precisamente na Mesa 5.1 "Direito Autoral e Proteção de Dados", no dia 5 de novembro de 2020 <https://codaip.gedai.com.br/>. A extensão do texto corresponde ao limite máximo estabelecido pela Organização do evento. Assim, apenas acrescentei, em notas de rodapé, hiperligações para as Fontes citadas, enquanto o aparato bibliográfico foi reduzido ao mínimo, remetendo quase só para publicações minhas recentes e com versões acessíveis em aberto na Internet, nas quais constam referências mais completas.

[402] Professor Adjunto de Direito Empresarial do IPBeja – Instituto Politécnico de Beja, em Portugal, lecionando sobretudo matérias de Direito Intelectual, de Proteção de Dados e de Cibersegurança em Graduação e Mestrado; no IPBeja, é também o Encarregado da Proteção de Dados e integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática. Pertence à EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência Europeia de Polícia e ao Grupo de Missão "Privacidade e Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, de Portugal. No Brasil, faz parte do Grupo de Trabalho de Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo, assim como das Comissões de Direito Digital da Seção de Santa Catarina e da Subseção de Campinas, assim como à Comissão de Inovação, Gestão e Tecnologia da Subseção de Guarulhos, todas da Ordem dos Advogados do Brasil <https://orcid.org/0000-0001-8861-0337> / <masseno@ipbeja.pt>.

1. o objeto: os dados não pessoais

Desde há quase uma década, os dados, tanto os pessoais quanto os não pessoais, sobretudo se armazenados e tratado em massa (*Big Data* / Megadados), passaram a ser uma fonte essencial de valor económico. Um valor acrescentado resultante das otimizações de recursos e das análises que permitem, inclusive de natureza preditiva, ao serem associados a algoritmos de Inteligência Artificial, designadamente pela "aprendizagem de máquina". Como é repetido *ad nauseam*, os dados foram qualificados como "o novo petróleo", para usar uma expressão cunhada por ocasião do Fórum Económico Mundial (*WEF* - Davos), em 2012. Embora a utilização generalizada, e em muitas ocasiões a despropósito desta metáfora, tenha levado o próprio *WEF* a marcar as diferenças em 2019, distinguindo claramente a informação, replicável um número indeterminado de vezes, dum recurso natural finito[403].

Ainda em termos preliminares, é de recordar que, na União Europeia, vigoram dois Regulamentos com uma especial relevância para o nosso objeto: o 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 (Regulamento Geral sobre a Proteção de Dados) – o RGPD, e menos conhecido Regulamento (UE) 2018/1807, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia – o RLFD[404].
Como resulta do Direito Primário da União Europeia, o RGPD assenta no Direito Fundamental à "autodeterminação informativa", enquanto projeção da "dignidade humana" [405]. Daí resultando que "Todas as pessoas têm direito à proteção dos dados de

[403] A propósito da "Economia dos Dados", das suas bases tecnológicas e de como as Políticas Públicas e Atos Legislativos a têm procurado promover e enquadrar na União Europeia, remeto sobretudo para as primeiras páginas, com as correspondentes anotações no texto indicado como (**2019b**).

[404] Para um acesso direto ao RGPD <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679> e também ao RFD < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>.

[405] Precisamente, no Artigo 2.º do *TUE – Tratado da União Europeia*, em cujos termos "A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem, incluindo os direitos das pessoas pertencentes a minorias. Estes valores são comuns aos Estados-Membros, numa sociedade caracterizada pelo pluralismo, a não discriminação, a tolerância, a justiça, a solidariedade e a igualdade entre homens e mulheres." e, ainda mais claramente, logo no Artigo 1.º da *Carta dos Direitos Fundamentais da União Europeia*, o qual assume que "A dignidade do ser humano é inviolável. Deve ser respeitada e protegida", com prioridade sistemática até perante o "Direito à vida", afirmado no Artigo 2.º. Uma versão consolidada e em Língua Portuguesa dos *Tratados* e da *Carta* está acessível neste endereço: <https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html>.

carácter pessoal que lhes digam respeito"[406] e, consequentemente, a apropriabilidade de dados pessoais está excluída, sendo estes dados qualificáveis como *res extra commercium*.

Não obstante, está garantido o "direito de portabilidade dos dados" pessoais, *rectius*, a possível transferência do seu tratamento dos dados para outro controlador, por iniciativa do "titular" e mantendo este todos os seus poderes e direitos, independentemente de existirem processadores ou outros destinatários dos dados[407]-[408]. Já o RLFD "aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais"[409], excluindo também os "dados não pessoais" conexos, isto é, sempre que "os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados", pois "o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679", nos termos do Artigo 2.º n.º 2 *in fine*.

Aliás, se o RGPD enuncia que "O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." (Considerando 26 *in fine*), já o RLFD esclarece que a fronteira entre os dados pessoais e os dados não pessoais é móvel, ou movediça, dependendo do evoluir das tecnologias de anonimização e de (re)personalização, mas assumindo os controladores os riscos de desenvolvimento inerentes[410]:

> "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. [Porém] Se os progressos tecnológicos permitirem transformar dados anonimizados em

[406] Assim, o Artigo 16.º do *TFUE - Tratado sobre o Funcionamento da União Europeia* e também, *ipsis verbis*, o Artigo 8.º da *Carta*, tal como ficaram depois do *Tratado de Lisboa*, assinado a 13 de dezembro de 2007 e em vigor desde 1 de dezembro de 2009.

[407] Neste sentido, dispõe o Artigo 20.º do RGPD. Embora não possamos ignorar a possibilidade de monetarização dos dados pessoais, como prevê, com limitações, o Artigo 3.º, n.ºs 1 e 8, da Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019L0770>. Entretanto, no dia 25 de novembro, já depois do *XIV CODAIP*, a Comissão Europeia apresentou a Proposta de Regulamento, do Parlamento Europeu e do Conselho, relativo à governação de dados (Regulamento Governação de Dados) (COM(2020) 767 final / 2020/0340(COD) <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0767>.

[408] Sobre estas matérias, remeto para o meu estudo (**2019b**), e bem assim para as referências aí presentes.

[409] Como consta no Artigo 2.º n.º 1, entendendo estes "na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679" (Art.º 3.º n.º 1), incluindo todos os relativos a "pessoa identificável [e] é considerada identificável uma pessoa singular [natural] 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".

[410] Para maiores desenvolvimentos, inclusive quanto às vias para a minimização dos riscos, sobretudo em termos preventivos, remeto para meu estudo (**2020a**), incluindo as correspondentes referências.

dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade."
(Considerando 9)

2. A atribuição de direitos sobre dados não pessoais

Como ponto de partida incontroverso, temos que os dados, só por si, não são passíveis de serem o objeto de direitos de natureza exclusiva, de uma propriedade /*property*, em qualquer aceção do termo. O mesmo ocorre com as "informações", entendendo estas como dados processados e dotados de sentido, com contexto, relevância e finalidade[411].

Dando continuidade uma metáfora que tenho por especialmente expressiva[412], no Oceano dos dados não pessoais temos um arquipélago duplo, o dos regimes de "Propriedade Intelectual". Os quais exigem, sempre e pelo menos, uma atividade criativa e apenas facultam respostas insulares. O que se verifica tanto em matéria de "Propriedade Industrial"[413], quanto na do Direito de Autor[414], e foi reiterado pelo *Acordo TRIPS*[415], fez um quarto se século.

O mesmo podemos concluir das iniciativas legislativas da União Europeia neste domínio. As quais, mesmo indo além dos limites marcados pelo *Acordo TRIPS*, só levaram a formação de marismas, com respostas parciais e inclusive movediças.

Antes de mais, temos a Diretiva das bases de dados[416]. A qual, mesmo não exigindo uma atividade criativa para a atribuição de um "direito *sui generis*" cujo objetivo, explícito

---

411 A propósito destas questões, na Doutrina portuguesa, ainda é de grande utilidade o texto de Dário Moura Vicente, aqui referido, ainda que uma parte das suas conclusões estejam superadas pela evolução das Fontes, como seria sempre de esperar atendendo à aceleração enformando estas tecnologias e as respostas normativas que as tentam acompanhar.

412 A qual orientou a minha comunicação à *Nordic Conference on Legal Informatics 2019,* realizada na Universidade da Lapónia em Rovaniemi, na Finlândia, em novembro de 2019, e, entretanto, publicada (**2020b**); embora uma versão maior e com referências para além das em Inglês já o houvesse sido antes em Língua Portuguesa, ainda que desprovida deste enquadramento metafórico (**2020a**).

413 Assim é, tanto na *Convenção da União de Paris para a Proteção da Propriedade Industrial*, de 6 de março de 1883, e suas atualizações <https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/dec22-1975.pdf>, quanto na *Convenção de Munique sobre a Patente Europeia*, de 5 de outubro de 1973 <https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/dec52-1991.pdf >.

414 Segundo a *Convenção da União de Berna para a Proteção das Obras Artísticas e Literárias*, de 9 de setembro de 1886, e suas atualizações <https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/dec73-1978.pdf>, e bem assim no *Tratado da Organização Mundial da Propriedade Intelectual sobre Direito de Autor*, de 20 de dezembro de 1996 <https://dre.pt/application/dir/pdf1sdip/2009/07/14600/0488904896.pdf>.

415 O *Acordo sobre os Direitos de Propriedade Intelectual Relacionados com o Comércio*, Anexo 1 C ao *Tratado de Marraquexe que cria a Organização Mundial do Comércio, seus anexos, decisões, declarações ministeriais e o Ato Final que consagra os resultados das negociações comerciais multilaterais do Uruguay Round*, de 15 de abril de 1994 <https://www.wto.org/english/docs_e/legal_e/27-trips.pdf>.

416 Pelos Artigos 7.º a 11.º da Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:PT:HTML>.

> "[…] consiste em garantir a proteção de um investimento na obtenção, verificação ou apresentação do conteúdo de uma base de dados durante o prazo limitado do direito." (Considerando 40)

assume que, apenas

> "[…] pretende salvaguardar a posição dos fabricantes de bases de dados relativamente à apropriação abusiva dos resultados do investimento financeiro e profissional realizado para obter e coligir o conteúdo, protegendo o conjunto ou partes substanciais da base de dados de certos atos cometidos pelo utilizador ou por um concorrente" (Considerando 39)

Consequentemente, é mantida a regra já aplicável às compilações de obras, ao excluir a acessão artificial dos dados, *maxime* das obras, constantes da base, pois

> "[…] a existência de um direito de se opor à extração e/ou reutilização não autorizadas da totalidade ou de uma parte substancial de obras, de dados ou de elementos de uma base de dados não origina um novo direito sobre essas mesmas obras, dados ou elementos." (Considerando 46)

Por sua vez, na Diretiva sobre o *saber-fazer* e os segredos de negócios[417], além de desligar a matéria da Concorrência Desleal, a União Europeia pretendeu facultar um meio adicional de proteção dos interesses empresariais, mormente dos das pequenas e médias empresas. Pois, se

> "A utilização de direitos de propriedade intelectual, como patentes, desenhos ou modelos ou direitos de autor, constitui um desses meios. Outro meio de apropriação dos resultados da inovação é a proteção do acesso e da exploração de conhecimentos valiosos para a entidade que não sejam do conhecimento geral. Esse valioso *know-how* e essas valiosas informações empresariais, que são confidenciais e que se pretende que permaneçam confidenciais, são designados como segredos comerciais."

Para tanto, quase confere direitos exclusivos a quem qualifica como "titular do segredo comercial", definindo-o como "a pessoa singular ou coletiva que exerce legalmente o controlo de um segredo comercial", pelo Artigo 2.º n.º 2.

Embora o faça com limitações tais que não permitem concluir da atribuição de direitos subjetivos sobre tais informações, sobretudo em função do disposto nos Artigos 3.º, 4.º e 5.º. Porém e mesmo que assim não fosse, os requisitos para a proteção de estas informações continuam sendo os já previstos no *Acordo TRIPS* e só estarão presentes em relativamente poucos casos[418].

---

[417] A Diretiva (UE) 2016/943, do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0943>.

[418] Especificamente, "a) serem secretas, no sentido de, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, não serem geralmente conhecidas pelas pessoas dos círculos que

Cumpre ainda acrescentar que, posteriormente e no âmbito do processo legislativo conducente à adoção do RLFD, a Comissão Europeia chegou a sugerir, entre outras de natureza contratual e como solução para os "dados gerados automaticamente", a instituição de um "Direito dos produtores de dados", entendido como [419]

> "[…] o direito de utilizar, e autorizar a utilização, de dados não pessoais poderia ser concedido ao «produtor de dados», ou seja, o proprietário ou utilizador a longo prazo (ou seja, o locatário) do dispositivo. Esta abordagem visaria esclarecer a situação jurídica e permitir um maior grau de escolha ao produtor de dados, dando aos utilizadores a possibilidade de utilizar os respetivos dados e, assim, contribuir para o desbloqueio dos dados gerados automaticamente. No entanto, haveria que especificar claramente as exceções aplicáveis, nomeadamente o fornecimento de acesso não exclusivo aos dados pelo fabricante ou pelas autoridades públicas, por exemplo para a gestão do tráfego ou por razões ambientais."

No entanto, porque não houve um acolhimento favorável por parte dos potenciais interessados, o RLFD omite uma tal possibilidade[420].

3. Mas, afinal, o "direito dos produtores de dados" sobreviveu…

Efetivamente e na sua versão final, o RLFD limita-se a colocar os parâmetros necessários para garantir a "portabilidade dos dados" dos dados não pessoais. Aliás e apesar das ambições iniciais presentes na Proposta, a efetividade das novas regras acaba por depender da autorregulação interprofissional e da adoção de códigos de conduta, embora o Regulamento determine uma atuação proativa da Comissão Europeia para a desencadear, no seu Artigo 6.º. Em termos metafóricos, apenas ficou uma… jangada.

Não obstante e até antes sua adoção, foi elaborado e assinado o *Código de Conduta sobre a partilha de dados agrícolas através de acordos contratuais na União Europeia*[421]. O qual foi assinado em Bruxelas, a 23 de abril de 2018, com o beneplácito do então Comissário Europeu para a Agricultura, Paul Hogan, e envolvendo a

---

lidam normalmente com o tipo de informações em questão, ou não serem facilmente acessíveis a essas pessoas; b) terem valor comercial pelo facto de serem secretas; [e] c) terem sido objeto de diligências razoáveis, atendendo às circunstâncias, para serem mantidas secretas pela pessoa que exerce legalmente o seu controlo", como enuncia o n.º 1 do Artigo 2.º da Diretiva, replicando o Artigo 39.º n.º 2 do *Acordo TRIPS*.

[419] Precisamente, na Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões "Construir uma economia europeia dos dados" (COM(2017) 9 final, de 10 de janeiro de 2017 <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0009>.

[420] Sobre as diversas questões tratadas neste ponto, remeto para as considerações e múltiplas referências de meu estudo (**2019a**).

[421] O qual não está disponível em Língua Portuguesa, mas pode ser consultado em Inglês <https://cema-agri.org/images/publications/brochures/EU_Code_of_conduct_on_agricultural_data_sharing_by_contractual_agreement_2020_ENGLISH.pdf >.

generalidade organizações profissionais e empresariais do setor agrícola, mesmo para além da agricultura em sentido restrito[422].

Aliás, a iniciativa resultou da circunstância de este setor estar entre os mais avançados e carecidos de regulação nestas matérias, como explicita o próprio RLFD:

> "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais […]. 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." (Considerando 9)

No que se refere aos seus conteúdos essenciais e em consonância com o RLFD, o *Código de Conduta* assume uma observância voluntária por parte dos associados das entidades signatárias, consistindo sobretudo num repositório das "melhores práticas", desde em perspectiva interprofissional consensualizada.

Quanto ao que mais no importa, temos que o mesmo tem por referência os "criadores de dados" ("data originators" / "owners"), isto é, "[…] the person or entity that can claim the exclusive right access to the data and control its downstream use or re-use". Uma criação que pode ocorrer de um modo direto ou por encomenda a terceiros.
Consequentemente, os dados produzidos em cada exploração agrícola pertencem ao respetivo empresário, devendo este beneficiar de todas as utilizações derivadas que vierem a ocorrer. Embora, as diversas indústrias, a montante ou a jusante da exploração, também sejam consideradas como "criadores de dados", mas nos respetivos âmbitos de atuação.

Por sua vez, os contratos celebrados devem salvaguardar o sigilo de todas as informações sensíveis sobre a exploração, assim como os direitos de propriedade intelectual ou sobre bases de dados não criativas envolvidos. Por isso mesmo, o acesso

[422] Designadamente, o *Código de Conduta* foi subscrito por entidades de alcance geral, como o Comité das Organizações Profissionais Agrícolas / Comité Geral da Cooperação Agrícola da União Europeia (COPA–COGECA) <https://copa-cogeca.eu/Menu.aspx> ou o Conselho Europeu de Jovens Agricultores (CEJA) <https://www.ceja.eu/home>, mas também por setoriais, tais como a Associação Europeia de Máquinas Agrícolas (CEMA) <https://www.cema-agri.org/> ou o Centro de Ligação Internacional dos Vendedores e Reparadores de Maquinaria Agrícola (CLIMMAR) <https://www.climmar.com/>, a Organização Europeia de Prestadores de Serviços Agrícolas, Rurais e Florestais (CEETTAR) <https://www.ceettar.eu/>, a Associação Europeia de Proteção de Culturas (ECPA) <https://croplifeeurope.eu/>, a *Fertilizers Europe* <https://www.fertilizerseurope.com/>, a, agora, *Euroseeds* <https://www.euroseeds.eu/>, o Fórum Europeu de Criadores de Animais (EFFAB) <https://www.effab.info/>, a Federação Europeia de Produtores de Rações (FEFAC) <https://fefac.eu/> ou ainda a *AnimalhealthEurope* <https://www.animalhealtheurope.eu/>.

aos dados só é lícito através de acordos explícitos, expressos e informados com os "criadores de dados", conforme ao definido contratualmente.

Além de ficar estabelecido que os "criadores de dados" não os cedem em exclusivo, salvo cláusula em contrário, e poderão sempre usá-los nas suas explorações. Nos mesmos termos, os "criadores de dados" poderão mudar de prestador de serviços de armazenamento e tratamento dos dados, concretizando assim a respetiva portabilidade. Porém, esta portabilidade deverá sempre salvaguardar as informações técnicas e os direitos intelectuais de terceiros, designadamente dos fornecedores de fatores de produção agrícolas, como máquinas, sementes ou agrotóxicos.

Finalmente, os contratos não poderão ser modificados sem acordo dos "criadores de dados". Em especial, no caso de haver um compartilhamento ou transmissão dos dados a terceiros, não previstas no contrato, os "criadores de dados" poderão opor-se, inclusive rescindindo o vínculo. Além de o contrato dever ser explícito e detalhado em matéria de responsabilidades, designadamente quanto à segurança dos dados.

4. As outras vias perspetiváveis desde a "Propriedade Intelectual"

Para terminar e de um modo muito breve, é necessário ter presente as atribuições de direitos de "Propriedade Intelectual" nos domínios da agrobiodiversidade e das biotecnologias agrícolas, as quais podem servir de referência para regulações. Aliás, as europeias respeitantes às variedades vegetais são expressamente mencionadas pelo *Código de Conduta* antes abordado.

Assim e no que se refere ao retorno financeiro para os "produtores dos dados", temos a *Convenção sobre a Diversidade Biológica* (CDB)[423], de 1992. Como é geralmente sabido, este instrumento internacional procura de garantir os interesses das comunidades [indígenas e] locais quanto à exploração por terceiros de recursos genéticos, e dos conhecimentos tradicionais com eles relacionados, em mão-comum, e não propriamente de direitos subjetivos atribuídos aos agricultores, mesmo tratando-se duma "espécie domesticada ou cultivada", Artigo 2.º. Quase duas décadas depois e nesta

[423] Na *Convenção sobre a Diversidade Biológica*, a qual foi assinada no Rio de Janeiro, a 6 de junho de 1992, por ocasião da Conferência das Nações Unidas sobre o Meio Ambiente e o Desenvolvimento, a qual ficou também conhecida por *Cimeira da Terra* ou por *Eco-92* <https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/dec21-1993.pdf>, sendo de nosso especial interesse o dispostos nos Artigos 1.º *in fine* e 15.º.

matéria, a *Convenção CBD* foi concretizada pelo *Protocolo de Nagoya*[424], já implementado na União Europeia[425].

Mais longe e prevendo os "direitos dos agricultores", incluindo o "direito de participar equitativamente na partilha dos benefícios resultantes da utilização dos recursos fitogenéticos para a alimentação e a agricultura", vigora o *Tratado da FAO sobre os Recursos Fitogenéticos*[426].

Por outro lado, temos a atribuição de direitos de reutilização nos próprios processos produtivos, como os presentes na *Convenção UPOV*[427] e no Regulamento europeu sobre as variedades vegetais[428], dos quais constam o denominado "privilégio do agricultor".

E ainda temos um "outro privilégio do agricultor", o previsto na Diretiva europeia sobre as invenções biotecnológicas[429], não só permitindo "utilizar o produto da sua colheita para proceder, ele próprio, à reprodução ou multiplicação na sua exploração", como também a "disponibilização do animal ou de outro material de reprodução animal para a prossecução da sua atividade agrícola, mas não a venda", oponíveis aos titulares dos direitos de patente, no seu Artigo 11.º, n.ºs 1 e 2[430].

---

[424] Por extenso *Protocolo sobre o acesso a recursos genéticos e a partilha justa e equitativa dos benefícios provenientes da sua utilização*, assinado em Nagoya, a 29 de outubro de 2010, o qual veio completar a *Convenção CDB* <https://dre.pt/application/conteudo/106589745>.

[425] Por força do Regulamento (UE) n. ° 511/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo às medidas respeitantes ao cumprimento pelo utilizador do Protocolo de Nagoia relativo ao acesso aos recursos genéticos e à partilha justa e equitativa dos benefícios decorrentes da sua utilização na União <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32014R0511>, completado pelo Regulamento de execução (UE) 2015/1866 da Comissão, de 13 de outubro de 2015, que estabelece normas de execução do Regulamento (UE) n.º 511/2014 do Parlamento Europeu e do Conselho no que respeita ao registo de coleções, à monitorização do cumprimento pelos utilizadores e às boas práticas <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32015R1866>.

[426] Mais precisamente, no Artigo 9.º do *Tratado Internacional sobre os Recursos Fitogenéticos para a Alimentação e a Agricultura*, da Organização das Nações Unidas para a Alimentação e a Agricultura (FAO), aprovado em Roma, a 3 de novembro de 2001 <https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/dec22-2005.pdf>.

[427] Assim, o Artigo 15.º n.º 3 da *Convenção Internacional para a Proteção das Obtenções Vegetais*, da União para a Proteção das Obtenções Vegetais (UPOV), aprovada em Paris, a de 2 dezembro de 1961, com a redação resultante ddesde o *Ato Adicional*, assinado em Genebra, a 19 de março de 1991 <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32005D0523>

[428] No Art.º 14.º do Regulamento (CE) n.º 2100/94 do Conselho, de 27 de julho de 1994, relativo ao regime comunitário de proteção das variedades vegetais <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31994R2100 >.

[429] A Diretiva 98/44/CE do Parlamento Europeu e do Conselho, de 6 de julho de 1998, relativa à proteção jurídica das invenções biotecnológicas <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31998L0044 >.

[430] Relativamente aos assuntos tratados neste ponto, remeto também para as considerações e referências de meu estudo (**2019a**).

5. Referências bibliográficas:

MASSENO, Manuel David.
____**Los datos no personales en las nuevas reglas europeas y su relevancia para los agricultores – Una Guía para el Estudio**. Rivista di diritto agrario. A. XCVIII – 3 (2019), pp. 586-613; também em RAMÓN FERNÁNDEZ, Francisca (Org.). Marco Jurídico de la Ciencia de Datos. Valencia: Tirant lo Blanc, 2020, pp. 301-329; no Brasil fora publicado em Campo Jurídico: Revista de Direito Agroambiental e Teoria do Direito, 7-2 (2019), pp. 122-144 <http://www.fasb.edu.br/revista/index.php/campojuridico/article/view/549> (**2019a**)

____ **Como a União Europeia procura proteger os cidadãos-consumidores em tempos de *Big Data***. Revista Eletrônica do Curso de Direito da UFSM 14(3):41708 (2019) <https://periodicos.ufsm.br/revistadireito/article/view/41708>; também em MARTINS, Guilherme Magalhães e LONGHI, João Victor Rozatti (Org.). Direito digital: direito privado e Internet (2020). 3.ª Ed. São Paulo: FOCO, pp. 409-428 (**2019b**)

____**Na borda: dados pessoais e dados não pessoais nos dois Regulamentos da União Europeia**. Cyberlaw by CIJIC, n. 9 (2020). Lisboa: Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, (**2020a**) <https://www.cijic.org/wp-content/uploads/2020/04/II_Na-Borda_Dados-Pessoais-e-nao-Pessoais-nos-2-regulamentos-da-UE_MDMasseno.pdf>; também em Marcos WACHOWICZ, Marcos (Org.). Proteção de Dados em Perspectiva: LGPD e RGPD na ótica do direito comparado. Curitiba: Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná (2020), pp. 126-145 (**2020a**).

____MASSENO, Manuel David. **On the waterfront: personal and non-personal data at both EU Regulations**. CARVALHO, Maria Miguel (Org.). E.Tec Yearbook - Artificial Intelligence & Robots. Braga: JusGov – Centro de Investigação em Justiça e Governação (2020), pp. 203-2012 <https://www.jusgov.uminho.pt/pt-pt/publicacoes/anuario-etec-2020-2/> (**2020b**)
VICENTE, Dário Moura. **A informação como objecto de direitos**. Revista de Direito Intelectual I (2014). Lisboa: APDI – Associação Portuguesa de Direito Intelectual, pp. 115-129.
Obs: Todas as hiperligações foram conferidas no dia 12 de janeiro de 2021.

Nos 20 anos da Carta Europeia dos Direitos Fundamentais: sobre a cultura dos direitos humanos como chão comum da União Europeia. Reflexões jurídico-políticas

Pedro Rebelo Botelho Alfaro Velez[431]

RESUMO

A proclamação política e a subsequente elevação a um plano jurídico vinculativo da Carta Europeia dos Direitos Fundamentais, foram marcos centrais na tentativa de construir uma União política europeia ancorada numa cultura comum de direitos humanos.
Por ocasião dos 20 da proclamação da Carta Europeia dos Direitos Fundamentais, refletir-se-á, de uma perspetiva político-jurídica, mais problemática do que dogmática, acerca do destino do projeto "constitucional" por ela simbolizado e veiculado[432].

PALAVRAS-CHAVE

Carta Europeia dos Direitos Fundamentais; direitos humanos; União Europeia; pós-liberalismo; federalismo americano.

[431] Professor da Universidade Europeia, Professor convidado no Instituto Politécnico de Leiria. Membro do centro de investigação CEDIS (Nova Direito). Nascido a 26.11.1979. Licenciado em Direito pela Faculdade de Direito da Universidade Nova de Lisboa (2002). Doutor em Direito (fevereiro de 2014), na especialidade de Ciências Políticas, também pela FDUNL. Nos últimos anos, tem-se dedicado à investigação e ao ensino, lecionando disciplinas de direito público (direito constitucional e direito administrativo) e de índole histórico-jurídica (história das instituições portuguesas, história do Estado), na FDUNL, na Universidade Europeia, na Escola de Direito da Universidade Católica Portuguesa-Porto, bem como no Instituto Politécnico de Leiria. Áreas de interesse: tipos históricos de Estado, formas políticas, regimes políticos/formas de governo e sistemas de governo, constitucionalismo, relações entre o político-constitucional e o religioso.

[432] O presente texto toma como base intervenção proferida no *Webinar* (11 dez. de 2020; 18-20h) intitulado *Nos 20 anos da Carta Europeia dos Direitos Fundamentais: sobre a cultura dos direitos humanos como chão comum da União europeia. Reflexões jurídico-políticas*, organizado no âmbito do *Privacy and Data Protection Centre* da Universidade Europeia, pelos Senhores Professores Doutores Cristina Gouveia Caldeira e Alexandre Sousa Pinheiro. Agradeço aos Senhores Professores a possibilidade de ter tomado parte no evento e ter podido refletir sobre temática jurídico-política de alcance civilizacional.

In the 20 years of the European Charter of Fundamental Rights: on the culture of human rights as the common ground of the European Union. Legal and political reflections

ABSTRACT

The political proclamation and the subsequent elevation to a binding legal plan of the European Charter of Fundamental Rights were central milestones in the attempt to build a European political Union anchored in a shared human rights culture. On the occasion, of the 20 years of the European Charter of Fundamental Rights proclamation, the reception of such a foundational project will be examined. It will be argued that its limitations have become more and more patent.

KEYWORDS

European Charter of Fundamental Rights; human rights; European Union; post-liberalism; American federalism.

Introdução

A solene proclamação política da Carta Europeia dos Direitos Fundamentais, a 7 de dezembro de 2000, e a sua posterior elevação, numa versão adaptada, a um plano jurídico vinculativo (por força do Tratado de Lisboa, que entraria em vigor no dia 1 de dezembro de 2009), foram marcos centrais da/na tentativa de edificação de uma União política Europeia explicitamente ancorada numa partilhada cultura dos direitos humanos.

As formulações preambulares tornavam – e tornam – patente um tal desígnio: «*Os povos da Europa, estabelecendo entre si uma união cada vez mais estreita, decidiram partilhar um futuro de paz, assente em valores comuns*», lia-se logo no primeiro parágrafo.

Pelo menos ao nível dos fundamentos proclamados, transparecia um compromisso com o específico discurso dos direitos inaugurado pela Declaração Universal dos Direitos Humanos (1948): «*Consciente do seu património espiritual e moral, a União baseia-se nos valores indivisíveis e universais da dignidade do ser humano, da liberdade, da igualdade e da solidariedade; assenta nos princípios da democracia e do Estado de direito*»[433].

I. As duas Europas

Ao referido momento convergente fundador, seguir-se-ia, porém, uma história de progressiva contraposição entre duas culturas distintas em sede de direitos fundamentais: entre uma cultura centrada numa ideia de autodeterminação (da vontade) individual ou pessoal; e uma outra atida a um certo *ethos* comunitário ou a uma certa "conceção do Bem" (para um utilizar um termo rawlsiano) tida como objetiva.

Prima facie, estará em causa uma crescente, e cada vez mais visível, divergência entre conjuntos de Estados; no limite, entre distintas zonas do continente europeu: genérica e caracteristicamente, Europa Ocidental versus Europa de Leste.

[433] Consultámos o(s) texto(s) constante(s) do Jornal Oficial da União Europeia (edição em língua portuguesa).

A Europa hiperliberal

Numa certa Europa, têm vindo a cristalizar novíssimos direitos ditos de autonomia ou de liberdade individual de escolha; direitos alcandorados a fundamentais, com incidência sobre as importantes e centrais dimensões antropológicas do começo e do fim da vida (humana), da configuração da família, da reprodução da espécie, da identidade corporal-sexual…[434]. Tudo representado como extensão do cânone "tradicional" dos direitos humanos, num processo que se afigura ainda *in fieri*[435].

Alguns exemplos recentes da afirmação desta dinâmica político-jurídica afiguram-se eloquentes: pense-se nas decisões dos tribunais constitucionais italiano, alemão e austríaco no que tange à problemática do fim de vida. O tribunal constitucional alemão invocou explicitamente a existência de um «direito subjetivo à morte»[436]. Num mesmo cumprimento de onda, o presidente do tribunal constitucional austríaco (Christoph Grabenwarter) sumariaria publicamente a doutrina subjacente à tomada de posição da jurisdição por si presidida: "A decisão plenamente consciente de cometer suicídio deve ser respeitada pelo legislador"[437].

Em amplos setores das classes político-mediáticas europeias, chega-se hoje ao ponto culminante de (meta)decretar como inquestionáveis estes novíssimos direitos de autodeterminação individual. O que talvez signifique um brutal estreitamento do campo das discussões e deliberações públicas e políticas tidas como razoáveis.

A Europa pós-liberal

Numa outra Europa, ao invés, registamos, desde logo, uma diferente paisagem no que toca aos referidos novíssimos direitos:

---

[434] Ver Rudi Di Marco, *Autodeterminazione e diritto,* Edizioni Scientifiche Italiane, Napoli, 2017.

[435] Processo esse que tem podido ser "descodificado" como manifestação acabada de uma noção de «*liberdade negativa*» (uma liberdade individual tendo apenas como critério a própria liberdade), que sempre tem acompanhado o discurso dos direitos humanos de derivação liberal; ver, neste sentido, Danilo Castellano, *Introducción a la filosofía de la política: Breve manual*, Marcial Pons, Madrid, 2020, pp. 113 e ss.

[436] Ver BVerfG, *Judgment of the Second Senate of 26 February 2020* - 2 BvR 2347/15 -, paras. 1-343, http://www.bverfg.de/e/rs20200226_2bvr234715en.html . Sobre a *sentenza n. 242/2019* do Tribunal Constitucional italiano, ver o comentário de Danilo Castellano e Rudi Di Marco, *Le motivazioni della Corte costituzionale sul suicídio assistito: ulteriore atto di "protezione dell'anarchia" da parte del giuspositivismo assoluto*, em *Filodiritto* (Filodiritto.com), 10 de dezembro 2019 (https://www.filodiritto.com/le-motivazioni-della-corte-costituzionale-sul-suicidio-assistito-ulteriore-atto-di-protezione-dellanarchia-da-parte-del-giuspositivismo-assoluto).

[437] Por decisão de 11 de dezembro de 2020, o referido tribunal considerou a lei austríaca criminalizadora da eutanásia violadora da Constituição, tendo a referida decisão constituído o legislador na obrigação de emanar lei descriminalização da eutanásia antes de janeiro de 2022. Ver www.fsspx.news/fr/news-events/news/la-cour-constitutionnelle-d'autriche-exige-une-loi-sur-l'euthanasie-62684.

A partir de 2001, a Europa dita liberal caminhou em direção à consagração da figura do casamento entre pessoas do mesmo sexo (em 2001, a Holanda terá sido o primeiro país europeu a consagrar a figura do casamento entre pessoas do mesmo, ano em que permitiu também a adoção por casais do mesmo sexo). Vários países do centro e do leste europeus, pelo contrário, não consagram sequer uniões civis abrangendo tais situações[438]. Não raro têm sido aprovadas emendas constitucionais no sentido de a afastar a redefinição do conceito tradicional de casamento[439]. Numa determinada comunidade política (Lituânia), o ordenamento jurídico bane inclusivamente o que define como «propaganda» *gay*[440].

Acresce que, em alguns países (Hungria, Polónia), assistimos mesmo à emergência de projetos político-constitucionais deliberada e declaradamente pós-liberais[441].

Na Hungria, parece estar *in fieri* a construção de uma ordem político-constitucional que tende a fundar-se numa ortodoxia pública "conservadora". A nova constituição húngara de 2011 é precedida de uma *invocatio Dei* – «Deus abençoe os Húngaros» – e de uma preambular «Confissão Nacional» *(sic)* evocando uma Nação concebida como unidade cultural intemporal de definição cristã; confissão nacional essa erigida a contexto interpretativo das concretas disposições constitucionais [artigo R (3)] Uma série de disposições constitucionais são particularmente significativas – assim, segundo o artigo L (1): «A Hungria protegerá a instituição do casamento como a união entre um homem e uma mulher estabelecida por decisão voluntária, e a família como a base da sobrevivência da nação»; segundo o Artigo II: «(A dignidade humana é

[438] Bulgária, Eslováquia, Letónia, Lituânia, Polónia, Roménia. Ver, na *Wikipedia*, a entrada *Recognition of same-sex unions in Europe* (https://en.wikipedia.org/wiki/Recognition_of_same-sex_unions_in_Europe).
[439] Foi o que ocorreu na Letónia (2005), na Croácia (desde 2013, na sequência de Referendo), na Eslováquia (2014), na Hungria (2012, como parte e parcela da adoção de uma nova constituição – ver *infra*). [Quer a Croácia, quer a Hungria, reconhecem legalmente, porém, "parcerias" entre pessoas do mesmo sexo]. Outras constituições pós queda do muro, consagram (Polónia) ou parecem consagrar (Lituânia) a dualidade de sexos como requisito essencial do casamento. No caso da Polónia, a disposição constitucional respetiva parece ter sido escrita com o intuito preventivo-defensivo de vedar à partida uma hipotética redefinição do conceito de casamento. Ver, de novo, a entrada referida na nota anterior.
[440] Sublinhando estes contrastes, ver *Charlemagne/The rainbow curtain*, em *The Economist*, 21 de novembro de 2020, p. 24.
[441] Não discutiremos se e até que ponto a nova ordem rompe ou tem vindo a romper com as normas político-constitucionais liberais-democráticas (no que tange à independência judicial ou à existência de uma imprensa livre, por exemplo), na direção de uma «democracia iliberal». Sobre esta questão, ver, entre nós, procurando um equilíbrio analítico, Carlos Blanco de Morais, *O Sistema Político – Em tempo de erosão da democracia representativa*, Almedina, 2017, pp. 172 a 176.

inviolável.) Todo o ser humano tem direito à vida e à dignidade humana; a vida embrionária e fetal devem ser objeto de proteção desde o momento da conceção»[442].

Na Polónia, a presente maioria governamental terá, porventura, como ideal condutor um horizonte político-constitucional similar (reatando hipóteses de estruturação político-constitucional debatidas no pós-queda do império soviético)[443].

A respeito da Polónia e do seu governo, é interessante registar que a anterior administração conservadora, em reação ao que entendeu serem os elementos de pendor "liberal-progressista" incorporados na Carta, negociou com sucesso a sua inclusão num protocolo ao Tratado de Lisboa relacionado com a aplicação da Carta Europeia dos Direitos Fundamentais (um dispositivo originalmente desenhado para o caso britânico e visando garantir a não sobre-extensão da jurisdição do Tribunal de Justiça da União Europeia; e cujas precisas implicações jurídicas têm sido discutidas, na doutrina e na jurisprudência)[444].

As duas Europas no interior de cada Estado

A duas culturas supramencionadas parecem separar Estados ou "áreas civilizacionais" do continente europeu; mas exprimem-se também no interior de cada Estado membro do conjunto político europeu, apenas variando a natureza e a intensidade das hegemonias em cada caso dominantes.

Já nos anos noventa, uma relevante contraposição entre o discurso católico dos direitos humanos – especialmente desenvolvido pelo Papa João Paulo II – e as interpretações seculares dos direitos humanos se tinha tornado eminentemente patente na vida político-constitucional de certas comunidades políticas europeias[445].

---

[442] Consultámos edição em inglês do Ministério da Justiça húngaro (2019).

[443] Para uma crítica global à presente ordem ocidental, provinda da atual classe governativa polaca, ver, de Ryszard Legutko, *The Demon in Democracy: Totalitarian Temptations in Free Societies*. Encounter Books, New York, NY., 2016 (devolvendo acusações de "iliberalismo" às democracias ocidentais, que hoje veiculariam uma forma mental totalizante…).

[444] *Protocolo (n.º 30) relativo à aplicação da Carta dos Direitos Fundamentais da União Europeia à Polónia e ao Reino Unido*. Ver, na *Wikipedia*, a entrada *Charter of Fundamental Rights of the European Union* (https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union).

[445] Sobre essa contraposição ver Gustavo Zagrebelsky, *El derecho dúctil, Ley, derechos, justicia*, trad., 10.ª ed., Editorial Trotta, Madrid, 2011, pp. 75 e ss. [Tradução espanhola de obra dos anos 90 que rapidamente adquiriu o estatuto de um clássico].

A militância da Comissão Europeia. O Parlamento Europeu como local de confronto entre visões jusfundamentais

As instituições europeias não têm ficado imunes à expressão das notadas trajetórias divergentes. Algumas das áreas dos novos direitos individuais ditos de autonomia ou de liberdade de escolha constituirão, à partida, é certo, áreas de reserva estadual (direito da família, por exemplo). A realidade jurídico-política "final" afigura-se, porém, mais complexa; pense-se, por exemplo, em recentes iniciativas da comissão europeia, no tocante a várias áreas: à liberdade de circulação de "situações familiares" definidas em certos Estados, mas não reconhecidas noutros; ao alargamento das definições de discurso de ódio online abrangendo a homofobia; ao corte de fundos europeus às cidades polacas autoproclamadas zonas livres de ideologia LGBT[446].

Ultimamente, o Parlamento Europeu tem vindo a tornar-se um palco de confronto entre as referidas visões jusfundamentais; segundo alguns em termos de crescente identificação dessa instituição com uma delas. Um momento parlamentar destes últimos tempos afigura-se particularmente eloquente: no princípio deste mês de dezembro, o Parlamento Europeu aprovou uma resolução «sobre a abolição de facto do direito ao aborto na Polónia» (*sic*), tendo condenado a decisão judicial suprema polaca que considerou inconstitucionais certas das poucas indicações legais justificando (foi o caso da malformação fetal, um tido de aborto tido por eugénico). A resolução estriba-se num reconhecimento explícito de um direito ao aborto como direito fundamental internacionalmente reconhecido (no âmbito dos direitos sexuais e reprodutivos)[447].

II. Paralelos com o cenário Americano

Seguindo a metodologia comparativa a que nos habituou o ilustre cultor do Direito Europeu professor Joseph H. H. Weiler, talvez se revele heuristicamente iluminante – em

[446] Ver, de novo, *Charlemagne/The rainbow curtain*, em *The Economist*, 21 de novembro de 2020, p. 24. Em relação à primeira das apontadas áreas objeto de iniciativa da Comissão, cumpre registar que o Tribunal de Justiça europeu teve já ocasião de nela entrar. Embora reconhecendo caber aos Estados Membros da União Europeia dispor sobre a definição do casamento, o Tribunal decidiu (5 de junho de 2018), porém, que «*o nacional de um Estado terceiro, do mesmo sexo do cidadão da União e cujo casamento com este último foi celebrado num Estado-Membro em conformidade com o direito deste, dispõe de um direito de residência superior a três meses no território do Estado-Membro de que o cidadão da União é nacional*». Segundo a instância jurisdicional europeia, a expressão cônjuge seria, no direito europeu chamado à colação, «*neutro do ponto de vista do género*». O acórdão em causa pode ser visto em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dab49a6ce70cfd42a3a61c9d52c93df497.e34KaxiLc3eQc40LaxqMbN4Pb3mLe0?text=&docid=202542&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=134584.

[447] A resolução está disponível em: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2876(RSP)&l=en

termos descritivos, prospetivos e prescritivos – lançar uma mirada à experiência norte-americana[448].

Também em solo americano se verifica a existência de marcados contrastes no que diz respeito à cultura dos direitos fundamentais.

De um lado um "discurso de direitos" – que tem sido um discurso de alargamento de direitos – girando em torno de uma certa compreensão de liberdade como autodefinição e autoexpressão do indivíduo. A conceção afirmada pelo Supremo Tribunal, a título de fundamento, em casos emblemáticos como o caso *Planned Parenthood of Southeastern Pennsylvania v. Casey* (de 1992)[449] – «*No coração da liberdade, está o direito de definir o nosso próprio conceito de existência, de sentido, do universo, e do mistério da vida humana*[450]» –; ou no mais recente *Obergefell v. Hodges* (2015)[451] – «*a Constituição promete liberdade a todos ao seu alcance, uma liberdade que inclui certos direitos específicos que permitem às pessoas, dentro de uma esfera legal, definir e expressar sua identidade*»[452].

Do outro, em contraponto, outras sensibilidades político-jurídicas, de orientação originalista ("historicista-americana") e/ou de pendor jusnaturalista[453]. A título de ilustração, tenha-se em conta o teor do trabalho produzido pela recente comissão estabelecida no âmbito Departamento de Estado – comissão liderada pela ilustre *scholar* e ex embaixadora dos EUA junto da Santa Sé (a católica Mary Ann Glendon, atualmente *Learned Hand Professor of Law at Harvard Law School*). Aí se sugere uma reancoragem do discurso dos direitos na lei natural – fala-se de «*direitos objetiva e universalmente verdadeiros*», por exemplo – , bem como uma depuração do catálogo de direitos

---

[448] Ver, por exemplo: Mauro Cappelletti, Monica Seccombe, and Joseph Weiler (eds.), *Integration through Law: Europe and the American federal experience. Vol. 1: methods, tools and institutions*, Walter de Gruyter and Co., New York 1986; J. Weiler, *Federalism Without Constitutionalism: Europe's Sonderweg*, em Kalypso Nicolaidis, Robert Howse (eds.), *The Federal Vision: Legitimacy and Levels of Governance in the United States and the European Union*, Oxford University Press, Oxford, 2001, pp. 54 a 70.

[449] Ver https://supreme.justia.com/cases/federal/us/505/833/case.pdf.

[450] «*At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life*».

[451] Ver https://www.supremecourt.gov/opinions/14pdf/14-556_3204.pdf. A natureza revolucionária da decisão do Tribunal levaria mesmo o célebre juiz Scalia a proclamar, em voto de vencido no referido caso, «*no social transformation without representation*». Sobre o pensamento jurídico-constitucional de Scalia, ver Robert P. George, *Antonin Scalia: An American Originalist*, em *Public Discourse*, 16. fev. 2016 (disponível em https://www.thepublicdiscourse.com/2016/02/16478/).

[452] «*The Constitution promises liberty to all within its reach, a liberty that includes certain specific rights that allow persons, within a lawful realm, to define and express their identity*».

[453] No discurso jurídico académico, ver, por exemplo, na revista *Public Discourse* (jornal online do "conservador" *Witherspoon Institute* – Princeton, New Jersey): Carson Holloway, *In Defense of Originalism*, 3 de abril de 2018 (https://www.thepublicdiscourse.com/2018/04/21097/) e, combinado as duas posições mencionadas no corpo do texto, Gerard V. Bradley, *Moral Truth and Constitutional Conservatism*, 10 fev. 2020 (https://www.thepublicdiscourse.com/2020/02/60037/).

fundamentais (insistindo-se em direitos tidos por essenciais ou primordiais – liberdade religiosa; propriedade); afastando-se outrossim um ideal de universalização-abstrata dos mesmos[454].

Perante o mencionado «choque de ortodoxias»[455], sugerem alguns, mais federalismo como resposta, em termos de uma deslocação das deliberações políticas atual e potencialmente fraturantes para os Estados federados[456].

III. Palavras finais. Do futuro Europeu

No que procede procurámos revisitar o projeto "constitucional" que terá estado na génese da Carta Europeia dos Direitos Fundamentais, tendo, porventura, sublinhado limitações que se têm vindo a tornar cada vez mais patentes.

Talvez se pudesse acrescentar, sugerindo uma camada extra de contextualização, que a Carta comportaria, sempre já, a possibilidade de distintas linhas de interpretação, dado o seu assumido minimalismo, mas também pela presença simultânea de distintos registos axiológicos (fundamentos personalistas; invocação das identidades e tradições nacionais; uma nova ideia abrangente de não discriminação). Não sem paralelos (ou continuidades) com a Declaração Universal dos Direitos do Homem (1948), cuja ambivalência (combinação de personalismos: um mais objetivista, com traços de jusnaturalismo clássico, outro mais subjetivista) tem sido notada, em sede de genealogia das diversas culturas de direitos atualmente existentes nas democracias ocidentais[457].

Em relação à Europa, talvez haja lugar para uma meditação análoga à que vimos ter sido sugerida no contexto americano como resposta ao desafio do "choque de ortodoxias". Aqui claro, não no sentido de mais federalismo, mas de manutenção – pelo menos – do existente protagonismo político dos Estados bem como de uma certa ideia de imparcialidade das instituições europeias (pelo menos das suas burocracias) ou de respeito, por parte dessas instituições, das identidades nacionais dos Estados-membros (para ecoar até as formulações do preâmbulo da Carta).

---

[454] Ver Commission on Unalienable Rights, *Report of the Commission on Unalienable Rights*, U.S. Departement of State, 2020 (https://www.state.gov/report-of-the-commission-on-unalienable-rights/)

[455] Para utilizar o título de um livro, com edição portuguesa, de um reputado constitucionalista e jusfilósofo de Harvard – Robert P. George, *Choque de Ortodoxias, Direito, Religião e Moral em Crise,* Edições Tenacitas, Lisboa, 2008.

[456] Ver Peter J. Leithart, *Is federalism the solution?* em *First Things*, 11. 6. 20 (https://www.firstthings.com/web-exclusives/2020/11/is-federalism-the-solution).

[457] Ver Grégor Puppinck, *Os Direitos do Homem Desnaturado*, Principia, Lisboa, 2019.

Tal será, porventura, condição da manutenção, como una, da atual União Europeia. Para além disso, se uma das visões dos direitos em contenda for canonizada ou privilegiada a nível Europeu, não ficará também prejudicada a existência de uma vida política plural (nos Estados e na União)? A força da União, já de si condicionante, somar-se-ia, em alguns casos, a preexistentes e constringentes hegemonias fácticas ou já situadas num plano constitucional de regime.

II_Outros Estudos

Google
Google Analytics - Mobile, Premium
www.google.com › analytics

Há mar e mar – Há plásticos e redes a pescar
Blue Circular PostBranding Project

Isabel Farinha[458]
Carlos A.M. Duarte[459]
Mafalda G. Carvalho[460]

RESUMO

O objetivo específico deste estudo é demonstrar, mediante a apresentação do projeto piloto - o Blue Circular Postbranding Project – o modo como a comunidade pode beneficiar de modelos de negócios circulares e que ferramentas de comunicação e design são necessárias para mudar as organizações nesta direção. Legisladores e reguladores, biólogos, designers, profissionais de marketing e publicitários são cruciais no processo de integração de uma prática de economia circular azul.

O *Blue Circular Postbranding Project* trabalha em estreita colaboração com o projeto "A Pesca para um mar sem lixo" da Docapesca Portos & Lotas e da Associação Portuguesa de Lixo Marinho (APLM). Projeto que funciona a dois níveis: prima tanto, pela promoção da sensibilização sobre o lixo existente no meio marinho como, se centra na remoção do lixo marinho dos oceanos com a colaboração dos pescadores. A colaboração entre os pescadores, as suas embarcações e os portos pesqueiros é importante para aumentar a conscientização das comunidades costeiras e pesqueiras e promover as atividades de corresponsabilidade por meio de uma abordagem a múltiplos stakeholders. Portugal, um país com uma longa tradição marítima e com um processo contínuo de extensão da sua plataforma continental, tem responsabilidades e obrigações em garantir a sustentabilidade dos oceanos: «Estamos a criar um movimento mobilizador» disse a ex-Ministra do Mar, Ana Paula

[458] Professora auxiliar do IADE-Universidade Europeia, PhD, especializada em Comunicação, Sociologia do Consumo, Marketing Escolar e Economia Circular Azul. Membro da UNIDCOM/IADE – Unidade de Investigação em Design e Comunicação e cocoordenadora do Projeto de Investigação & Inovação em Espaço Marítimo, 'Blue Circular Postbranding Project', suportado pelo Programa Operacional Mar2020 e apoiado pela Associação para o Desenvolvimento Sustentável da Região Saloia, A2S., Lisbon, Portugal *isabel.farinha@universidadeeuropeia.pt*

[459] Professor catedrático. Atualmente exerce a função de Vice-reitor para a área de Ensino e Formação, Internacionalização e Empregabilidade da Universidade Europeia e é membro da UNIDCOM/IADE – Unidade de Investigação em Design e Comunicação onde co-coordena o projeto de I&D "Blue Circular Postbranding Project", financiado pelo Programa Operacional Mar 2020 e apoiado pela A2S - Associação para o Desenvolvimento Sustentável da Região Saloia.*UNIDCOM/ IADE - Universidade Europeia, Lisbon, Portugal. carlos.duarte@universidadeeuropeia.pt*

[460] Mafalda Gil de Carvalho é Bióloga, pós-graduada em Animais e Sociedade e mestranda em Ciências do Mar. É colaboradora no Projeto de Investigação & Inovação em Espaço Marítimo – *Blue Circular Postbranding Project*, da UNIDCOM/IADE – Unidade de Investigação em Design e Comunicação da Universidade Europeia, como gestora de projetos. É a *Ocean Policy Manager* do projeto Ocean Hub Portugal, da 'Sustainable Ocean Alliance', e é líder ambiental no projeto *Generation Earth* da WWF Portugal.

Vitorino destacando a importância do Encontro dos Oceanos (Cardoso, 2018). Neste contexto, a 'Estratégia Europeia para o Plástico em Economia Circular', adotada em 16 de janeiro de 2018 (COM, 2018), e em particular o lixo marinho de origem marinha que é abordada com uma proposta específica de Diretiva sobre Instalações Portuárias de Receção visa transformar a forma como os produtos de plástico são concebidos, produzidos, usados e reciclados na UE. Neste sentido, são necessárias marcas que consigam gerir o consumo sustentável através de uma tecnologia que transforme os materiais descartáveis em matéria-prima reutilizável, sem renunciar à qualidade e ao design.

Em suma, ter uma abordagem de economia circular azul para este problema e os instrumentos de política e ferramentas de gestão corretos, tal como preconizado pelo *Blue Circular pb,* mostra ser absolutamente necessário para resolver a questão do consumo excessivo de bens. A metodologia SOSTAC (Smith, 2015) permitirá desenvolver os pontos cardeais da proposta de comunicação deste projeto com vista a uma convocatória a esta causa ambiental e social[461].

PALAVRAS-CHAVE

Consumo sustentável, cidadania, causa social, proteção ambiental, economia circular azul.

ABSTRACT

The specific aim of this study is to demonstrate through a pilot project – *Blue Circular Postbranding Project* - different ways in which the community can benefit from circular business models and which communication and design tools are needed to shift organizations in this direction. Legislators and regulators, biologists, designers, marketers and advertisers are most crucial in the process of mainstreaming a blue circular economy practise.

The *Blue Circular Postbranding Project* woks in collaboration with the "Fishing for a sea without litter" project, from the Portuguese Port Authorities (Docapesca Portos & Lotas) and the non-profit/non-governmental organisation Portuguese Association of Marine Debris (APLM). It works on two levels by providing bins to fisherman: on the one hand, promoting awareness about the garbage in the marine environment and on the other, focused on the removal of marine litter from the oceans. Collaboration between fishermen, their vessels and fishing ports is important for raising awareness among coastal communities, fishing communities and promoting co-responsibility activities using a multi-stakeholder approach. Having a circular economy approach to this problem and the right policy instruments and management tools, as the *Blue circular pb* aims, are absolutely needed to address the issue of overconsumption of goods.

KEYWORDS

Sustainable consumption, citizensship, social cause, environmental protection, blue circular economy.

[461] Ficha técnica em anexo.

Introdução

"Neste último meio-século o planeta Terra sofreu a sua mais acelerada e qualitativa transformação em muitos milhões de anos, podendo a causa dessa metamorfose ser atribuída a uma única e singular causa: o incansável metabolismo da nossa espécie, transformando a complexa pluralidade da Natureza em homogénea simplicidade, isto é, em mercadorias consumíveis, energia, calor, lixo e entropia".

Viriato Soromenho-Marques *in* Jornal de Letras, 23 de setembro de 2020, p.28

A problemática dos plásticos no mar surgiu, pela primeira vez, na agenda internacional na década de 60 do seculo passado, devido à ingestão de produtos plásticos por aves marinhas e é, hoje, compreendido como um dos principais problemas transfronteiriços, pelo que a "solução" para a poluição marinha por plástico requer cooperação internacional (Brink *et al.,* 2016). Um mecanismo legalmente vinculativo a nível global poderia superar alguns desafios da governança de plásticos marinhos, no entanto, o direito internacional é baseado no consentimento de todas as partes do acordo (Henkin, 1979), mas o processo de elaboração do tratado permite que as partes "pesem os benefícios e encargos do compromisso e explorem, redefinam e, às vezes, descubram os seus interesses" (Chayes & Chayes, 1993).

A produção global de plástico em 2017 foi de cerca de 335 milhões de toneladas (Plastics Europe, 2018) e as estimativas de 2014 preveem uma duplicação da produção global de plástico em 20 anos (Ellen MacArthur Foundation, 2016). Esta poluição marinha por plástico tem consequências sobre o meio ambiente e a biodiversidade, assim como em indústrias, tais como as do turismo, a da navegação e a da pesca, e representa um risco potencial para a segurança alimentar e a saúde humana (Barboza *et al*., 2018).

O lixo marinho pode ser definido como "qualquer material sólido persistente, fabricado ou processado que foi descartado, abandonado e, eventualmente, acaba por atingir o ambiente marinho ou costeiro" (Watkins *et al.* 2016). A maior parte do lixo

marinho abrange embalagens e pequenos pedaços de plástico ou poliestireno não identificáveis (Chen, 2015) que provém, principalmente, de fontes terrestres. Estima-se, igualmente, que 4,8 a 12,7 milhões de toneladas de plástico chegaram aos oceanos de terra em 2010 (Jambeck *et al.*, 2015), sendo que, cerca de 80% do despejo de plástico nos oceanos vem de países em desenvolvimento, incluindo a China, a Indonésia, as Filipinas, o Vietnam e o Sri Lanka (Jambeck & Geyer 2015), onde os sistemas de coleta e recuperação não estão adequadamente equipados para lidar com grandes quantidades de resíduos (Ellen MacArthur Foundation, 2016) (Fig 1). O lixo marinho proveniente de fontes marítimas, é composto especialmente por artes de pesca perdidas ou descartadas, como as chamadas "redes fantasmas".

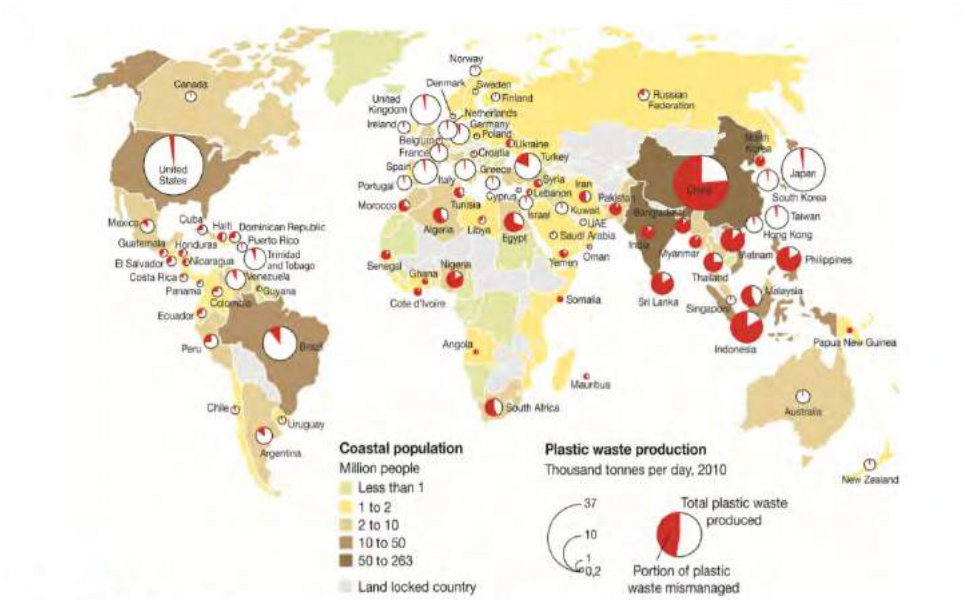


Fig. 1 Poluição por plásticos de diferentes populações. Adaptado de Jambeck & Geyer 2015.

Perante este cenário, é imperativo proceder à criação de alternativas à acumulação desenfreada de plásticos no oceano, por base de uma economia azul circular.

1. Projeto de economia circular azul

"Neste momento, a economia circular é um desígnio civilizacional, um dos principais desafios da década. Por isso, é certo que a regulação será cada vez mais exigente e que esta será uma oportunidade de negócio crescente para as empresas, que terão clientes, investidores e colaboradores cada vez mais exigentes, a querer que os produtos que consomem não sejam os melhores do mundo, mas os melhores para o mundo".

João Wengorovius Meneses, Secretário-Geral do BCSD Portugal

A Assembleia das Nações Unidas para o Meio Ambiente (UNEA-2), que teve lugar em Nairobi em maio de 2016 emitiu uma resolução de alto nível para priorizar o combate ao lixo marinho (UNEP 2016). Na reunião do G7, em Bona, em maio de 2015, os líderes mundiais também se comprometeram a lidar com o lixo marinho. A *meta 14.1* dos Objetivos de Desenvolvimento Sustentável para 2030 exige uma redução significativa da "poluição marinha de todos os tipos, em particular de atividades terrestres, incluindo detritos marinhos" até 2025 (Brink *et al*., 2018).

Fig. 2 Objetivos de desenvolvimento sustentável, focando a meta 14.1 de redução da poluição marinha (ODS 2016-2030).

Algumas das orientações compreendidas neste *objetivo 14* (Fig. 2) é a prevenção e redução de lixo marinho; a limitação do impacto da pesca no meio marinho e adaptação da pesca à proteção das espécies; a promoção da proteção, restauração e gestão sustentável dos ecossistemas marinhos e costeiros, assim como, da biodiversidade marinha; fomentar o desenvolvimento local das comunidades costeiras; aumentar o conhecimento científicos, desenvolver capacidades de investigação e de tecnologia marinha; entre outros.

Ao nível da União Europeia (UE), a Diretiva Quadro da Água da UE (60/2000 / CE) e a Diretiva Quadro da Estratégia Marinha da UE (2008/56 / CE) incluem disposições sobre a redução da poluição e do lixo marinho, respetivamente. Com o lançamento do Plano de Ação da Economia Circular, a Comissão Europeia comprometeu-se a "adotar uma estratégia para os plásticos na economia circular, abordando questões como a reciclabilidade, a biodegradabilidade, a presença de substâncias perigosas em determinados plásticos e lixo marinho" (COM/2015/0614) (Brink *et al*., 2018).

Existem várias iniciativas regionais e internacionais para combater o lixo marinho que são relevantes para a Europa. Estes incluem a Declaração de Lanzarote (2016), o

Compromisso de Honolulu (2011), MARPOL, a Convenção de Londres, uma série de Convenções Marítimas Regionais (por exemplo, Barcelona, OSPAR) e outras iniciativas regionais, como o Plano Regional Mediterrâneo sobre Lixo Marinho (2014) (Brink *et al*., 2018). Já o G20 deve promover a transição para uma economia circular a fim de criar um sistema de plástico que funcione a longo prazo, com maior eficácia do sistema, maior produtividade dos recursos e redução drástica do lixo marinho (Brink *et al*., 2018).

Relativamente ao objetivo *número 12*, este visa a produção e consumo sustentável e compreende inúmeras orientações, de entre as quais, o desenvolvimento da economia circular com enfoque na desmaterialização, economia colaborativa e consumo sustentável, conceção de produtos, uso eficiente e valorização de recursos; a alteração dos modelos de produção e consumo; o aumento das taxas de recolha, reciclagem e calorização globais e setoriais para os diferentes materiais constituintes dos resíduos; a promoção das práticas de compras públicas, ecológicas e sustentáveis, entre outros (Fig. 3).

Fig. 3 Objetivos de desenvolvimento sustentável, focando o objetivo *número 12* (ODS 2016-2030).

Existe um amplo conjunto de ferramentas e opções para evitar o lixo marinho, seguindo-se, para isso, uma hierarquia de medidas preventivas a montante até medidas de limpeza a jusante. Geralmente, as medidas a montante são preferíveis às medidas a jusante, no entanto, todas são necessárias (pelo menos a curto e médio prazo) para lidar com o lixo marinho (Watkins *et al.,* 2016) (Fig. 4).

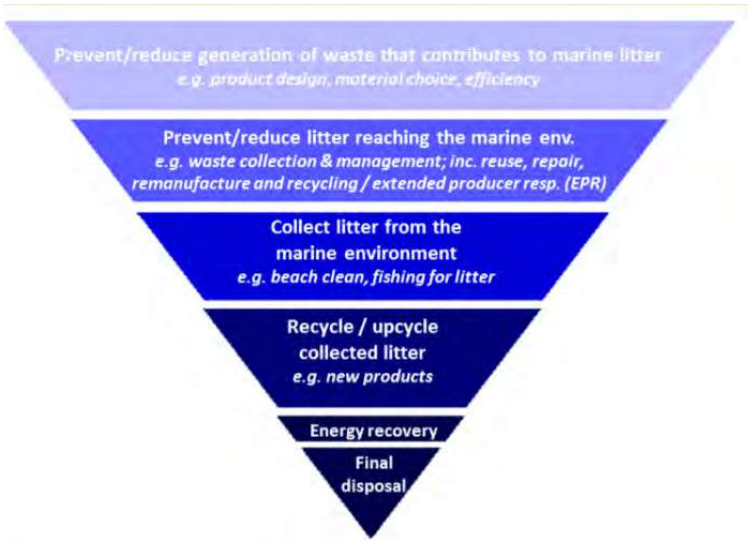


Fig. 4 Esquema de uma hierarquia para a gestão do lixo marinho.
Figura adaptada de Watkins *et al.,* 2016.

Já que, tudo é fluído na pós-modernidade e, também no universo das marcas assim o é, a nossa conceção de *post branding*, as matérias-primas são continuamente reinventadas.

O *Blue Circular Post Branding Project* é, nesta visão, uma proposta de Economia Circular Azul (APA, 2016; APA 2018) em que o desperdício de recursos é recriado em novas marcas por um processo de transição e de participação ativa que motivados os atores da cadeia de valor. Desde os produtores aos consumidores e alicerçado em I&D, aposta-se numa abordagem sistémica, multidisciplinar, colaborativa e de design promotora de soluções sustentáveis como alavanca para a mudança ambiental e social.

Iniciativas como esta, proporcionadas pela candidatura A2S/Mar2020, para além de procurarem criar emprego e potenciar novos mercados para o lixo marinho reciclado, consciencializam sobre estas temáticas, e tentam evitar pressões sobre o meio marinho. As nossas áreas de intervenção são em Cascais, estendendo-se até ao Estoril; e em Mafra, desde a Ericeira até à Encarnação. De forma a poder executar esta ideia, encontrámos parceiros cujos ideais se alinham com os nossos, tais como, Docapesca/ APLM (Associação Portuguesa do Lixo Marinho) - Projeto " A Pesca por um Mar sem Lixo"; Associação para o Desenvolvimento Sustentável da Região Saloia (A2S); Câmara Municipal de Mafra; Ericeira Business Factory; Tratolixo; Câmara Municipal de Cascais/ Cascais Ambiente, entre outros (Fig. 5).

Fig. 5 Área da intervenção do *Blue Circular pb nos* portos de pesca de Cascais e Mafra e alguns dos parceiros do projeto.

2. Estratégia de I&D na promoção do património ambiental das zonas pesqueiras e costeiras

O *Blue Circular Postbranding Project* centra a sua atividade nos portos de pesca de Cascais e da Ericeira, sendo um projeto-piloto na Capitania de Cascais. Nestes portos, a comunidade piscatória é convidada a colocar, quer as redes e os artefactos de pesca, quer o lixo marinho (plásticos e demais detritos), recolhido a bordo das suas embarcações em Ecopontos Marítimos criados para o efeito. Este é um projeto de Investigação & Inovação em Espaço Marítimo que pretende, a partir do lixo marinho, produzir artigos duradouros com impacto ambiental, social, visual e de consumo consciente.

O *Blue Circular pb* decorre em parceria com o projeto "A Pesca por um Mar sem lixo" promovido pelo Ministério do Mar e desenvolvido pela Docapesca/ Associação Portuguesa do Lixo Marinho (APLM). Este, visa melhorar a gestão de resíduos a bordo das embarcações de pesca e sensibilizar os pescadores para a importância da adoção ou manutenção das boas práticas ambientais. Promovem, igualmente, a recolha dos resíduos gerados a bordo e capturados nas artes de pesca e disponibilizam infraestruturas adequadas para a sua receção. Este projeto tem, portanto, por base a união dos pescadores e dos portos de pesca de modo a melhorar as condições ambientais da zona costeira e a preservação dos ecossistemas marinhos portugueses.

Na fase inicial de desenvolvimento deste projeto, e para que os pescadores nos auxiliem na recolha e lixo marinho, foram colocados ecopontos no Porto de Cascais, de modo a que ocorra lá a deposição destes resíduos. Os ecopontos estão identificados, sendo uns deles apenas para redes e cordas de pesca e outros apenas para materiais plásticos diversos. De mencionar que há dois pontos que dispõem destes ecopontos: Porto de Cascais (Ecoponto marítimo); Porto de Pesca de Cascais (Cais dos Aprestos) (Fig. 6).

Fig. 6 Lançamento das iniciativas EcoPonto Marítimo, Pesca por um Mar sem Lixo e Blue Circular PostBranding Project a 14 de julho de 2020 e Localização e exemplificação fotográfica dos Ecopontos

Este projeto visa a promoção de um mundo com menos lixo e desperdício pela poupança de matérias-primas escassas; a redução da deposição de resíduos, encarada como opção de fim de linha; um aproveitamento dos recursos físicos e humanos pelo reforço do papel das comunidades de pescadores no desenvolvimento e na governação dos recursos locais da pesca e das atividades marítimas; um forte contributo para a preservação ambiental das zonas costeiras e do património marinho e visa, igualmente, a promoção da saúde pública. Depois da coleta, é necessário realizar um processo de avaliação qualitativo do lixo (Fig. 7), para que possa ser encaminhado para cadeia de valor acrescentado (Tratolixo).

Fig. 7 Processo de transformação de PET para produção de fibras de poliéster.

A missão do projeto é fomentar, a partir do lixo marinho (plásticos e redes de pesca) uma produção de artigos duradouros com impacto ambiental, social, visual e de consumo consciente. Pretende-se, também, estimular um processo transparente e integrado de economia circular potenciando um desenvolvimento socioeconómico assente no princípio de "eu compro o que é nosso" e potenciar a sustentabilidade, por base de um processo ético e criativo de design focado num elevado padrão de qualidade e de consciência ambiental.

Já relativamente aos objetivos do projeto, estes baseiam-se na transmissão da ideia de que, ao abrigo de um processo transparente, há vida no plástico recolhido dos oceanos, (re)transformando-o em novos produtos. O *Blue Circular Postbranding Project* no âmbito duma abordagem de economia circular azul, que envolve a academia, a comunidade piscatória, a sociedade civil, a esfera política e empresarial, tem como meta, a metamorfose do lixo diariamente descartado em algo novo e com valor acrescentado capaz de promover um consumo consciente e globalmente sustentável (Fig. 8).

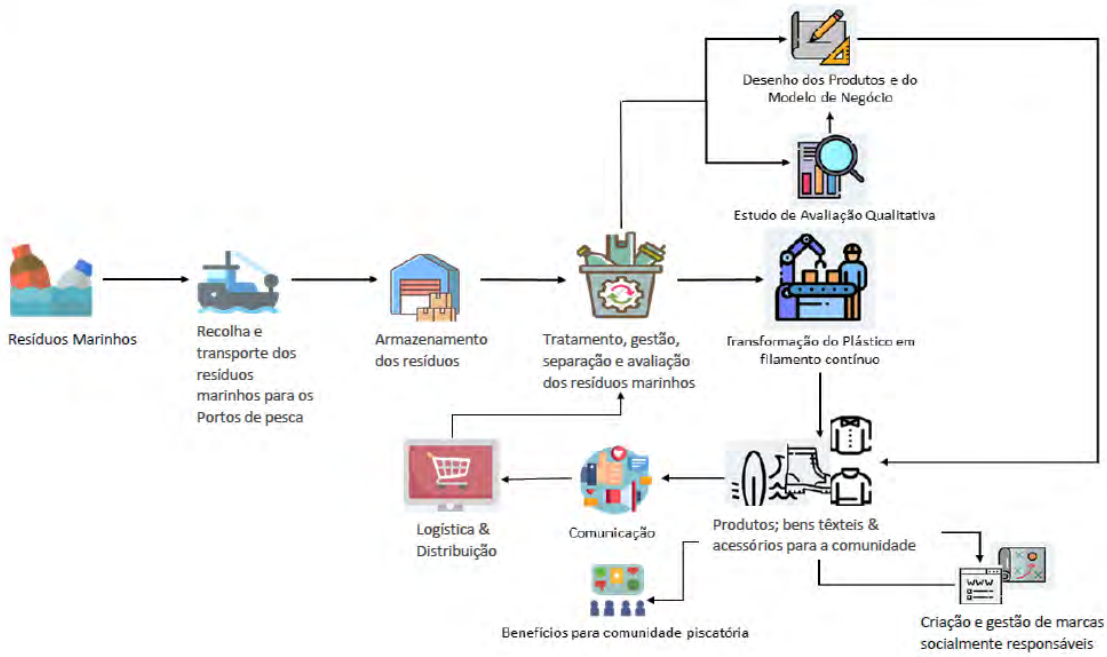


Fig. 8 Esquematização do projeto e das etapas que acarreta.

Relativamente às etapas do processo, detalha-se a coleta, a purificação do plástico originando o *pellet*, a transformação do *pellet* a filamento, a produção de têxteis a partir destes filamentos (Fig. 9).

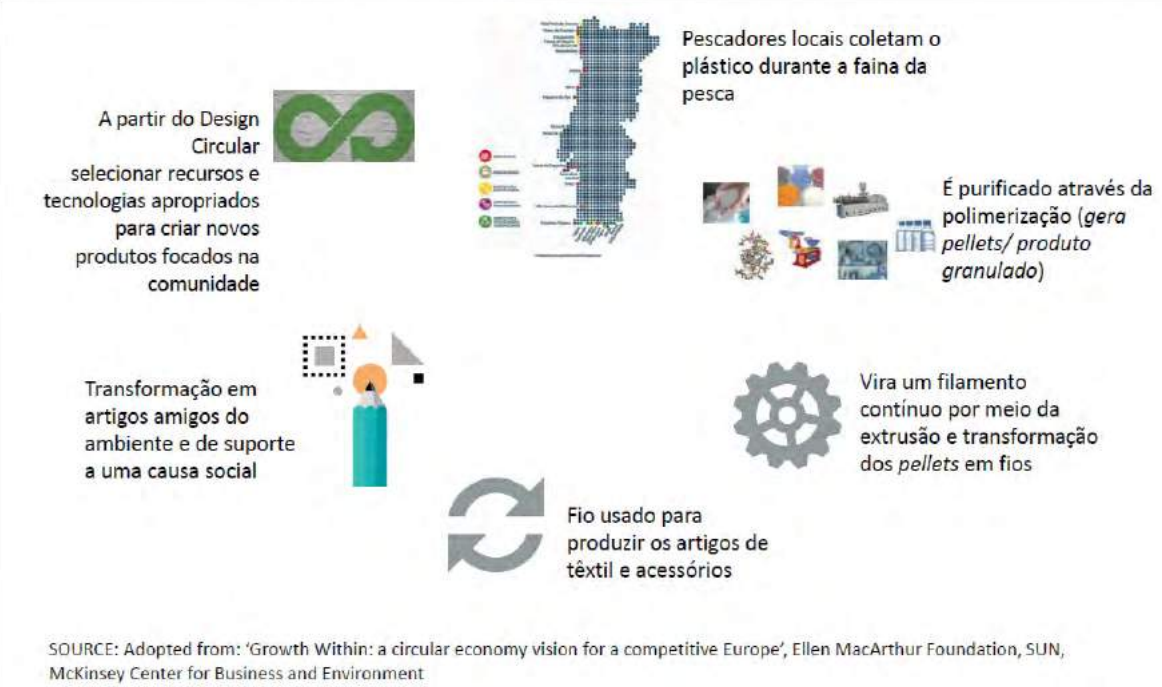


Fig. 9 Esquematização das etapas no caso português.

O projeto conta, também, com o apoio de diversas organizações em diversos setores, de entre as quais:

Recolha, gestão e tratamento de resíduos- Tratolixo; Plasoeste

Incubação- Ericeira Business Factory; ID:Co.Lab; Now_Beato

Indústria- Falcão Fibras; LMA (Leandro Manuel Araújo, S.A.)

Associações - Brigada do Mar; Ajude a Limpar a Praia (ALP)

I&D- Sociedade de Geografia de Lisboa (Secção de Geografia dos Oceanos).

Outras das atividades que são pretendidas implantar por este projeto-piloto, compreendem designadamente: o fomento de workshops de capacitação que visem difundir ferramentas de comunicação, *networking*, partilha de experiência e de boas práticas no âmbito da literacia dos oceanos; a discussão e divulgação da pesquisa em fóruns/conferências nacionais e internacionais; a organização de uma exposição/conferência pública internacional dedicada à importância estratégica da Economia Circular Azul; a preparação e direção de estudos críticos em revistas nacionais e internacionais da especialidade; elaboração de artigos e, a disponibilização na Web de

uma mediateca -base de dados, documentação e material audiovisual relevante reunida com vista a futuros estudos (Portal do Projeto).

3. Ativação do modelo de design circular

De acordo com a ex-Ministra do Mar, Ana Paula Vitorino (Cardoso, 2018), é necessária uma crescente sensibilização em todos os países sobre a importância dos oceanos e da Economia Azul, defendendo o "oceano como fator importante na sobrevivência do nosso planeta", pelo que, passando a citar, "o oceano trilhará o rumo de uma Economia Azul, caso as nações demonstrem o compromisso necessário para abraçar esse grande desafio, explicou a líder da pasta do Mar. No fundo, o oceano revelará a resposta: os governos e as comunidades empresariais terão sim, de revolucionar a forma como o abordam".

Sobre o lixo marinho, a ex-Ministra do Mar afirmou que vários países já começaram a combater "um problema que é de todos nós": alertando para a urgência da transformação da forma e do ritmo através dos quais 'produzimos' lixo. Ana Paula Vitorino vê ainda na economia circular "um pilar das próximas décadas" e a resposta ideal para contrariar o paradigma ainda vigente que urge alterar. "Temos de ter cadeias de valor para transformarmos o lixo" em novos produtos e novas matérias, concretizou (Cardoso, 2018).

A economia circular apresenta uma série de soluções para lidar com o lixo marinho nos oceanos (Atualidade Parlamento Europeu, 2020, dezembro 14). Incluem, a saber, redução de material, design para reciclabilidade no final da vida, análises do ciclo de vida de química verde e o uso de matérias-primas de base biológica (Barnes *et al.* 2009). Há algumas *Startups* a trilhar o seu caminho neste campo, no entanto, muitas das que fazem o design em Portugal vão buscar as matérias-primas a outros países longínquos. Assim sendo, se formos a considerar a pegada carbónica que tal implica, desde as emissões de combustíveis fósseis desde o ponto de recolha (suponhamos Índia), até ao local onde são elaborados os *pellets* e, consequentemente, as fibras (suponhamos Eslovénia), para que depois sejam enviadas para o país a realizar o design (suponhamos Portugal) é absurdamente elevado[462].

Assim sendo, o que pretendemos é realizar estes processos todos em Portugal, de modo a que, estes sejam realmente sustentáveis, minimizando a pegada carbónica a larga escala, consciencializando e potenciando a literacia do oceano, assim como, criando mais

[462] Tomando como exemplo o da marca "Conscious The Label".

emprego e mais oportunidades no nosso país. De forma a efetivar esta ideia, pretendemos abranger um público-alvo bastante alargado, como é passível de ser averiguado na Fig. 10.

Fig. 10 Esquematização do público-alvo que será envolvido no projeto.

4. Conclusão

As ações dos setores público e privado que apoiam a transição para uma economia circular fornecem uma estrutura para simultaneamente aumentar a eficácia do sistema de plásticos por meio de um projeto melhor, aumentar sua produtividade de recursos e reduzir as externalidades negativas dos plásticos, incluindo, as do lixo marinho e os seus impactos (Brink *et al*., 2018).

Muitos países desenvolveram estratégias de eficiência de recursos e economia circular que integram objetivos para transformar o setor de plásticos e, simultaneamente, reduzir o lixo marinho (Brink *et al*., 2018).

O Plano de Ação da União Europeia para a Economia Circular (Comissão Europeia, 2018) compromete a Comissão Europeia a ajudar a reduzir os impactos do lixo marinho, aumentando ao mesmo tempo, o valor dos materiais na economia da UE. Espera-se que uma futura Estratégia sobre "Plásticos na Economia Circular" se torne um

dos principais veículos para lidar com o lixo marinho na UE (Brink *et al.*, 2016), recorrendo e cumprindo os ODS, nomeadamente o *número 12 e 14*.

De acordo com o discurso que a antiga Ministra do Mar proferiu em 2018, aquando da conferência sobre a "Nova fase de descobertas", há a reter uma mensagem de compromisso, ambição e cooperação como requisitos essenciais para o sucesso dos sectores ligados, direta e indiretamente, ao Mar.

> "São os países que tomam as decisões quando convergem. Vamos deixar-nos de conversas e vamos assumir compromissos para uma nova política do oceano, um desígnio que tem de ser encarado como uma missão e não como *business as usual*"
>
> Ana Paula Vitorino (Cardoso, 2018)

O *Blue Circular Postbranding Project*, enquanto projeto-piloto, compromete-se, assim, a desenvolver um trabalho que tem por intuito abranger, tanto o campo social, envolvendo os pescadores na recolha de lixo marinho; como o estabelecimento de parcerias entre associações/instituições/empresas que tenham uma visão similar à nossa para que juntos consigamos alcançar o pretendido, ou seja, a minimização máxima de plástico nos ecossistemas marinhos; a que se associa o domínio da inovação, de modo a explorar a transformação destas matérias-primas em *pellets* e, consequentemente, em fibras têxteis para execução de produtos duradouros e, por fim mas não menos importante, o campo de design, que conferirá a estas peças de plástico reutilizado funções específicas e sustentáveis, de estética inigualável.

5. Referências

Agência Europeia do Ambiente. (2016). *Circular economy in Europe—Developing the knowledge base.* European Environment Agency. Retrieved from https://www.eea.europa.eu/publications/circular-economy-in-europe

Agência Europeia do Ambiente. (2018). *The circular economy and the bioeconomy - Partners in sustainability*. European Environment Agency. Retrieved from https://www.eea.europa.eu/publications/circular-economy-and-bioeconomy

Atualidade Parlamento Europeu. (2020, dezembro 14). *Economia circular: definição, importância e benefícios - Infografia animada*. Retrieved from https://www.europarl.europa.eu/news/pt/headlines/economy/20151201STO05603/economia-circular-definicao-importancia-e-beneficios.

Autoridade de Gestão do MAR2020. (2019). Programa Operacional Mar 2020. *O Que é o MAR2020.* Retrieved from http://www.mar2020.pt/o-que-e-o- mar-2020/

Barboza, L., Vethaak, A., Lavorante, B., Lundebye, B., & Guilhermino, A. (2018). Marine microplastic debris: An emerging issue for food security, food safety and human health. *Marine Pollution Bulletin,* pp. 336-348.

Barnes, D., Galgani, F., Thompson, R., & Richard, C. (2009). Accumulation and fragmentation of plastic debris in global environments. *Philosophical Transactions of the Royal Society B: Biological Sciences,* pp. 1985-1998.

Blue Circular Postbranding Project. (2020). Retrieved from https://bluecircular.org/

Brink, P., Schweitzer, J.P., Watkins, E., & Howe, M. (2016). Plastics Marine Litter and the Circular Economy. *Institute for European Environmental Policy for the MAVA Foundation,* pp. 1-17.

Brink, P. (2018). Circular economy measures to keep plastics and their value in the economy, avoid waste and reduce marine litter. *Economics Discussion Papers*, No. 2018-3

Cardoso, B. F. (2018, junho 26). Fase «de novas descobertas»: Ministra do Mar aponta o rumo da nova Economia Azul sustentável e inovadora. *Marítimo.* Retrieved from https://revistacargo.pt/ministra-economia-azul-circular/

Cascais. (2020, julho 14). *Mar sem lixo*. Retrieved from https://www.cascais.pt/noticia/mar-sem-lixo

Chayes, A., & Hayes, A. (1993). On compliance. *International Organization*, vol. 47, issue 2, pp. 175-205

Chen, C. (2015). Regulation and Management of Marine Litter. *Marine Anthropogenic Litter,* pp. 395-428.

COM (2018). União Europeia. Comunicação da Comissão Ao Parlamento Europeu, Ao Conselho, Ao Comité Económico e Social Europeu e Ao Comité Das Regiões. *Uma Estratégia Europeia para os Plásticos na Economia Circular*. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52018DC0028

Crippa, M., Wilde, B., Koopmans, R., Leyssens, J., Muncke, J., Ritschkoff, A-C., Van Doorsselaer, K., Velis, C., & Wagner, M. (2019). A circular economy for plastics: Insights from research and innovation to inform policy and funding decisions. *Publications Office of the European Union: Luxembourg.*

Ellen Macarthur Foundation. (2016). Rethinking the future of plastics: the new plastics economy. *Ellen Macarthur foundation,* pp. 1-120

European Commission. (2019). *A circular economy for plastics – Insights from research and innovation to inform policy and funding decisions*, *Publications Office of the EU.* Retrieved from *https://op.europa.eu/en/publication-detail/-/publication/33251cf9-3b0b-11e9-8d04-01aa75ed71a1/language-en/format-PDF/source-87705298*

European Commission. (2020). *The EU Blue Economy Report. 2020.* Publications Office of the European Union. Luxembourg. Retrieved from https://blueindicators.ec.europa.eu/sites/default/files/2020_06_BlueEconomy-2020-LD_FINAL-corrected-web-acrobat-pro.pdf

Henkin, L. (1979). *How Nations Behave*. Published for the Council on Foreign Relations. New York: Columbia University Press.

Hudson, A. (2018, novembro 26). United Nations Development Programme. *Blue Economy: a sustainable ocean economic paradigm*. Retrieved from https://www.undp.org/content/undp/en/home/blog/2018/blue-economy-sustainable-ocean-economic-paradigm.html

Jambeck, J., & Geyer, R. (2015). Plastic waste inputs from land into the ocean. Science 347.

Meneses, J. W. (2020, setembro). Diretrizes da Sustentabilidade - Economia Circular: Legislação e standards internacionais. BCSD Portugal. Retrieved from https://bcsdportugal.org/diretrizes-da-sustentabilidade-economia-circular-setembro-2020/

Ministério dos Negócios Estrangeiros. (2017). Relatório nacional sobre a implementação da Agenda 2030 para o Desenvolvimento Sustentável, pp. 86-88.

National Geographic. (2018 June). *Planet or Plastic? We Made Plastic. We Depend on it. Now We're Drowning in it.* Retrieved from https://www.nationalgeographic.com/magazine/2018/06/plastic-planet-waste-pollution-trash-crisis/

ODS. (2017). *Objetivos de Desenvolvimento Sustentável, 2016-2030 (ODS)*. Relatório nacional sobre a implementação da Agenda 2030 para o Desenvolvimento Sustentável – Portugal. Retrieved from https://unric.org/pt/objetivos-de-desenvolvimento-sustentavel/

Plastics Europe. (2018). *Plastics – the Facts 2018: An analysis of European plastics production, demand and waste data*. Retrieved from https://www.plasticseurope.org/application/files/6315/4510/9658/Plastics_the_facts_2018_AF_web.pdf

DGPM - Direção-Geral de Política do Mar. (2020). Retrieved from https://www.dgpm.mm.gov.pt/

Projeto "A Pesca para um mar sem lixo", Docapesca Portos & Lotas, S.A. e Associação Portuguesa de Lixo Marinho (APLM). Retrieved from http://www.docapesca.pt/pt/comunicacao/noticias/item/mar-sem-lixo.html

Smart Waste Portugal. (2020). Pacto Português para os Plásticos. Retrieved from http://www.smartwasteportugal.com/pt/atividades/pacto-portugues-para-os- plasticos

Smith, P. (2011). *SOSTAC® Guide To Writing The Perfect Plan*. V1.1, Kindle Edition.

Soromenho-Marques, V. (2020, setembro 23). Outro Planeta Terra: da Exuberância à Agonia. *Jornal de Letras*, p.8.

UNEP (2016). *UN Environment Annual Report 2016 – UNEP. Engaging People to Protect the Planet*. Retrieved from.https://www.unenvironment.org/annualreport/2016/index.php?page

Watkins, E., Gionfra, S., Schweitzer, J., Pantzar, M., Janssens, C., & Brink, P. (2017). EPR in the EU Plastics Strategy and the Circular Economy: A focus on plastic packaging. *Institute for European Environmental Policy for the MAVA Foundation.*

ANEXO - FICHA DO PROJETO BLUE CIRCULAR POSTBRANDING PROJECT

CANDIDATURA A CONCURSO A2S/ MARE2020:

Projeto De Investigação & Inovação em Espaço Marítimo

COORDENADORES CIENTÍFICOS E COORDENADORES DO PROJETO:

COORDENADORES CIENTÍFICOS/ INVESTIGADOR RESPONSÁVEL - Carlos Duarte (PhD), UNIDCOM/IADE – Universidade Europeia e Isabel Farinha (PhD), UNIDCOM/IADE – Universidade Europeia

COORDENADORES CIENTÍFICOS - Rui Miguel (PhD) da Universidade da Beira Interior (Unidade de Investigação FibEnTech/ Universidade parceira).

IDENTIFICAÇÃO DO BENEFICIÁRIO:

EUROPEIA ID - Associação para a Investigação em Design, Marketing e Comunicação

IDENTIFICAÇÃO DA OPERAÇÃO:

Código da Operação [MAR-04.03.01-FEAMP-0294]; Medida: Aumentar o emprego e a coesão territorial (DLBC)

SÍNTESE DOS ELEMENTOS REFERENTES À DECISÃO DE APROVAÇÃO:

Data de inicio e de fim do projeto - 16 de dezembro de 2019 a 15 de dezembro de 2021.

III_Legislação e Jurisprudência Comentadas

Acórdão do Tribunal de Justiça da União Europeia relativo ao Processo C-311/18, de 15 de julho de 2020 (*Schrems II*)

Alexandre Sousa Pinheiro[463]

COMENTÁRIO

Neste trabalho vamos analisar a decisão designada como Schrems II do Tribunal de Justiça da União Europeia (TJUE) conjuntamente com as conclusões do Advogado-Geral. Ponderaremos o futuro das transferências de dados pessoais para Estados não dotados de proteção adequada nos termos do Regulamento Geral sobre Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho 27 de abril de 2016, publicado a 4 de maio - RGPD464) e da Diretiva 95/46/CE465 e, nesse contexto, o papel das standard contractual clauses (SCCs). Seguir-se-á, na terminologia da decisão, a análise das "garantias adequadas" (appropriate safeguards) exigidas a responsáveis pelo tratamento e a subcontratantes para a transferência de dados pessoais para Estados terceiros que não disponham da garantia de proteção adequada nos termos do artigo 45.º do RGPD.

[463] Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa (2012), onde foi Professor até 2019. É atualmente Professor de Direito Administrativo na Universidade Europeia e membro da CADA (Comissão de Acesso aos Documentos Administrativos). Advogado (desde 1993). Consultor na Presidência do Conselho de Ministros e no Ministério da Justiça (1995-2002). Vogal da Comissão Nacional de Proteção de Dados (2001-2006), tendo sido membro das Autoridades Comuns de Controlo da EURODAC e do EUROJUST. Na Presidência Portuguesa do Conselho da União Europeia (2007) preside ao MGD (*Multidisciplinary Group on Organised Crime*). Consultor Principal do CEJUR (2006-2009). Coordenador Científico do Projeto Legis-Palop (2009 – organização da legislação dos Estados Africanos de Língua Portuguesa). Senior Expert da Agência Europeia de Direitos Fundamentais (2008-2011). Consultor da Assembleia da República para matérias de Técnica Legislativa (2013-2014). Coordena o Curso Avançado de Proteção de Dados (2012-2017) e exerce funções como Juiz Arbitral no Tribunal Arbitral do Desporto (2015-2018) e de Juiz-Presidente nos Colégios Arbitrais do Conselho Económico e Social. É Coordenador do *Privacy and Data Protection Centre.* Autor de cerca de 60 títulos e participante regular em iniciativas públicas de Direito Público e Proteção de Dados.

[464] JO 2016, L 119, p. 1.

[465] *J O 1995 L 28 p. 0031.*

I. As conclusões do Advogado-Geral

1. Começamos por avaliar a posição do Advogado-Geral em *Schrems II* - Henrik Saugmandsgaard Øe (19 de dezembro de 2019), que não foi, no essencial, seguida pelo TJUE, tal como ocorreu na área da proteção de dados, com a posição do Advogado-Geral Niilo Jääskinen no Processo C-131/12, de 13 de maio de 2014 (Google Spain SL e Google Inc. vs. *Agencia Española de Protección de Datos* [AEPD] e Mario Costeja González)[466] [467].

Em *Schrems II* a posição do Advogado-Geral relativamente ao *Privacy Shield* (aprovado pela Decisão de Execução [UE] 2016/1250 da Comissão de 12 de julho de 2016) está, essencialmente, centrada em a questão da validade da decisão não ter sido explicitamente levantada pelo *Data Protection Commissioner* (DPC) irlandês, pelo que não caberia ao TJUE decidir sobre a questão (165).

O Advogado-Geral sustenta que a avaliação da validade da Decisão *Privacy Shield* pelo TJUE seria uma decisão imprudente (182) por não permitir que através da tramitação interna o DPC considerasse não se poder pronunciar sobre a queixa de Maximilliam Schrems sem a apreciação da validade do da referida Decisão, podendo recorrer para os tribunais nacionais, a fim de que estes procedessem ao competente reenvio prejudicial (180).

Apesar de esta consideração basilar, o Advogado-Geral expandiu a sua posição relativamente à validade da Decisão *Privacy Shield* (196 e seguintes), concluindo que tem dúvidas quanto à conformidade da Decisão relativa ao *Privacy Shield* com o artigo 45.º do RGPD interpretado à luz dos artigos 7.º, 8.º e 47.º da Carta Europeia de Direitos Fundamentais da União Europeia (CEDFUE) e do art.º 8.º da Convenção Europeia de Direitos Humanos (CEDH) (342).

O n.º 3 da Decisão *Privacy Shield* sobre o Acesso e a Utilização de Dados Pessoais transferidos ao abrigo do *Privacy Shield* de proteção da privacidade EU-EUA pelas Autoridades Públicas dos EUA, refere no considerando 64 que:

---

[466] "Conclusões do advogado-geral Niilo Jääskinen apresentadas em 25 de junho de 2013. Processo C-131/12", disponível em: https://op.europa.eu/en/publication-detail/-/publication/36af7add-c149-11e3-86f9-01aa75ed71a1/language-pt/format-PDF/source-search.

[467] Observação de Marc Rotenberg, "From Snowden to China. Toward a new alignement on transatlantic data Protection", European Law Journal, Volume: 26, 2020, p. 147.

"Tal como decorre do anexo II, secção I, ponto 5, a adesão aos princípios limita-se ao necessário para observar os requisitos de segurança nacional, interesse público ou aplicação da lei."

A validade da Decisão *Privacy Shield*, segundo o Advogado-Geral estaria dependente de saber se o ordenamento jurídico dos Estados Unidos asseguraria, relativamente a dados transferidos da UE, um nível de proteção contra as ingerências no exercício dos seus direitos fundamentais «substancialmente equivalente» ao garantido nos termos do RGPD e da CDFUE, em domínios excluídos do âmbito do direito da União, dos seus compromissos ao abrigo da CEDH (247).

Neste contexto importa apreciar o Considerando 109, da Decisão *Privacy Shield*:

"(…) nos termos da secção 702 da FISA (*Foreign Intelligence Surveillance Act*), o FISC (*Foreign* Intelligence *Surveillance Court*) não autoriza medidas de vigilância individuais; em vez disso, autoriza programas de vigilância (tais como o PRISM e o UPSTREAM) com base em certificações anuais elaboradas pelo *Attorney General* e o *Director of National Intelligence*. A secção 702 da FISA permite que se visem pessoas que se acredite estarem localizadas fora dos Estados Unidos a fim de obter informações no estrangeiro. Esta seleção da pessoa visada é realizada pela NSA (*National Security Agency*) em duas fases: em primeiro lugar, os analistas da NSA identificaram os cidadãos de países terceiros localizados no estrangeiro cuja vigilância conduzirá, com base na avaliação do analista, às informações externas relevantes especificadas na certificação. Em segundo lugar, após a identificação destas pessoas e a sua aprovação como objetivos por um amplo mecanismo de análise no âmbito da NSA, são designados (ou seja, desenvolvidos e aplicados) os seletores que identificam os meios de comunicação (como o endereço de correio eletrónico) utilizados pelas pessoas visadas. Tal como indicado, as certificações a aprovar pelo FISC não contêm informações sobre as pessoas visadas, mas sim categorias de identificação das informações no estrangeiro. Embora o FISC não avalie — com base numa causa provável ou em qualquer outra norma — se as pessoas são adequadamente visadas para efeitos de obtenção de

informações externas, o seu controlo alarga-se à condição de que «um objetivo significativo da recolha consiste na obtenção de informações no estrangeiro. Com efeito, nos termos da secção 702 do FISA, a NSA pode recolher comunicações de cidadãos de países terceiros fora dos EUA apenas se for possível considerar razoavelmente que um determinado meio de comunicação está a ser utilizado para comunicar informações no estrangeiro (por exemplo, relacionadas com terrorismo internacional, proliferação nuclear ou atividades cibernéticas hostis). As determinações para este efeito são objeto de controlo jurisdicional. As certificações também necessitam de prever procedimentos de orientação e minimização. O *Attorney General* e o *Director of National Intelligence* verificam a conformidade e os serviços são obrigados a comunicar todas as situações de incumprimento ao FISC (bem como ao Congresso e à *Intelligence Oversight Board* do Presidente), que, com base no que precede, pode alterar a autorização."

As conclusões do Advogado-Geral apresentam interpretações diferenciadas das previstas no considerando citado, referindo, nomeadamente que as medidas de vigilância previstas não incluem garantias de limitação das pessoas que podem ser objeto de medidas de vigilância e das finalidades para que pode verificar-se recolhas de dados pessoais em circunstâncias substancialmente equivalentes às que são exigidas pelo RGPD interpretado à face dos artigos 7.º e 8.º da CDFUE (301).

2- Relativamente às SCCs, o Advogado-Geral conclui não se encontrar fundamento para as considerar inválidas (343).

Os atos da Comissão em causa são: (i) Decisão 2001/497/CE da Comissão, de 15 de junho de 2001, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva [95/46][468]; (ii) Decisão 2004/915/CE da Comissão, de 27 de dezembro de 2004, que altera a Decisão [2001/497] no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros [469]; e (iii) Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais-tipo aplicáveis à

[468] JO 2001, L 181, p. 19
[469] JO 2004, L 385, p. 74

transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho [470].

O Advogado-Geral, na análise da validade das SCCs centra-se, fundamentalmente, na sétima questão prejudicial, que questiona a compatibilidade da Decisão 2010/87 com legislação da UE. Está em causa a ausência de fixação de obrigações a Estados terceiros para os quais tenha havido transferência de dados pessoais ao abrigo das SCCs (121).

Assim, existe a necessidade de interpretar as SCCs em conformidade com a legislação da UE, particularmente com o RGPD, antes que se decida no sentido da existência de invalidade.

Aí, o Advogado-Geral faz notar que as SCCs se baseiam no cumprimento do artigo 46.º, n.2, alínea c) do RGPD e que a aferição da existência de garantias adequadas para a transferência deve ser analisada em cada situação concreta (126). Desta forma, a Decisão 2010/87 deve ser interpretada em conformidade com os artigos 7.º, 8.º e 47.º da CDFUE, não devendo concluir-se no sentido da sua invalidade (127).

3. Com brevidade, concluímos que a posição do Advogado-Geral se integra numa perspetiva de proteção do sistema de transferências de dados para Estados terceiros, anterior a *Schrems II.*

Se, por um lado, considera que as SCCs devem ser avaliadas caso a caso sem que se identifique razão de invalidade, entende não se dever pronunciar, de forma absoluta, sobre a Decisão *Privacy Shield*, embora a leitura atenta das conclusões caminhe no sentido de considerar que existe violação da CDFUE, do RGPD e da Diretiva 95/46/CE. Pensamos que a posição do Advogado-Geral, bem como posteriormente a do TJUE foi no sentido de não deixar a UE e o Espaço Económico Europeu (EEE) desprovido de meios gerais destinados a garantir a transferência de dados para Estados terceiros.

A incompletude das SCCs é compatível com a exigência imposta pelo artigo 46.º, n.2, alínea c) do RGPD [471].

Neste sentido, pode observar-se o Considerando 108 do RGPD:

[470] JO 2010, L 39, p. 5.
[471] Ver anotação de Alexandre Sousa Pinheiro e Carlos Jorge Gonçalves ao artigo 46.º in Alexandre Sousa Pinheiro (coordenador), Cristina Pimenta Coelho, Tatiana Duarte, Carlos Jorge Gonçalves e Catarina Pina Gonçalves, "Comentário ao Regulamento Geral de Proteção de Dados", Almedina, Coimbra, 2018, pp. 512 e ss.

> "Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade (…)."

Aceita-se que cláusulas provindas de garantias autorizadas pelas autoridades de controlo, nos termos do artigo 58.º, n.º 2, alínea g) do RGPD (124) constituam uma forma de integração de lacunas de decisões aprovadas pela Comissão. Não existem razões de cariz procedimental ou relacionadas com a natureza dos atos aprovados pela UE que se oponha a esta conclusão.

Neste sentido, não deve ser esquecida a jurisprudência do TJUE – no essencial *Schrems I,* que veremos *infra* - que permitiu às autoridades de controlo fiscalizar a compatibilidade de decisões da Comissão com a CDFUE e com a legislação da UE.

Como conclusão pensamos que as conclusões do Advogado-Geral são atravessadas por uma ponderação de consequências de carater jurídico-político e não apenas de índole dogmática.

Outra solução é inviável em temas com a complexidade e os reflexos práticos da transferência de dados pessoais para Estados terceiros.

II. Acórdão Schrems II

4. O Acórdão *Schrems II* entrou para o panteão das grandes decisões do TJUE em sede de proteção de dados no dia em que foi conhecido.

Por se viver uma crise sanitária, multiplicaram-se os webinários de apresentação da decisão e de auscultação das consequências futuras da invalidade da Decisão *Privacy Shield.*

Até há data não existe ainda uma sólida doutrina constituída, mas foram já tomadas posições por órgãos da UE, bom como por autoridades de controlo nacionais (DPAs).

Cabe notar que o Acórdão *Schrems II* tem um forte amparo em *Schrems I* que teve como consequência direta a invalidade da Decisão da Comissão *Safe Harbor* (Decisão da

Comissão de 26 de Julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de *Safe Harbor* e pelas respectivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* dos Estados Unidos da América)[472].

5. No Processo C-362/14, de 6 de outubro de 2015 (*Schrems I*)[473], o TJUE dispôs da Diretiva 95/46/CE como parâmetro normativo, tendo sido apreciada a competência das autoridades de controlo nacionais para examinar queixas de particulares questionando a validade de decisões da Comissão respeitantes à atribuição a Estados terceiros do estatuto proteção adequada ao abrigo do artigo 28.º da Diretiva (37).

O TJUE interpretou as competências das autoridades nacionais de controlo (artigo 28.º) nos termos do artigo 8.º, n.º 3 da CDFUE, determinando que, apesar de não estarem em causa tratamentos de dados realizados no território de um Estado membro o âmbito da fiscalização abrange a transferência de dados para Estados terceiros (47).
O TJUE, enunciando uma delimitação negativa, expressou que o artigo 8.º, n.º 3 da CDFUE e o artigo 28.º da Diretiva não continham restrições à competência das autoridades nacionais para examinar transferências de dados pessoais para países terceiros que tenham sido objeto de uma decisão da Comissão de acordo com o artigo 25.º, n.º 6, desta diretiva (54).

> O considerando 60 apoia o entendimento sustentado:
> "Considerando que, em todo o caso, as transferências para países terceiros só podem ser efetuadas no pleno respeito das disposições adotadas pelos Estados membros nos termos da presente diretiva nomeadamente do seu artigo 8.º ".

5.1. Relativamente à validade da Decisão *Safe Harbor*, o TJUE refere que do artigo 25.º, n.º 6 da Diretiva 95/46 resulta que é a ordem jurídica do Estado terceiro que deve assegurar um nível de proteção adequado (74).

[472] JO L 215, p. 7
[473] Para uma análise desta decisão, ver Domingos Soares Farinho, "(Un)Safe Harbor: Comentário à decisão do TJUE C-362/14 e suas consequências legais", Forum de Proteção de Dados, CNPD, n.º 2, 2016, pp. 108 e ss.

O TJUE cita a Comunicação da Comissão ao Parlamento Europeu e ao Conselho COM (2013) 847 final [474], que, com significativa relevância, assinala os problemas materiais da Decisão *Safe Harbor*:

> "Desde que foi adotado em 2000, o sistema «porto seguro» tornou-se um vetor para o fluxo de dados pessoais entre a UE e os EUA. A importância de dispor de uma proteção eficaz no caso de transferências de dados pessoais tem vindo a aumentar devido ao aumento exponencial dos fluxos de dados, cruciais para a economia digital, bem como aos enormes progressos realizados a nível da recolha, do tratamento e da utilização dos dados. As empresas da Internet como a Google, Facebook, Microsoft, Apple e Yahoo, possuem centenas de milhões de clientes na Europa e transferem dados pessoais destinados a ser tratados nos EUA numa escala impensável no ano 2000. As deficiências verificadas a nível da transparência e da aplicação do acordo contribuem para perpetuar os seguintes problemas específicos, que deverão ser abordados: (a) Transparência das políticas de proteção da vida privada adotadas pelos membros do sistema «porto seguro», (b) Aplicação efetiva dos princípios de proteção da vida privada pelas empresas nos EUA e (c) Eficácia da sua aplicação. Além disso, o acesso em grande escala pelos serviços de informações a dados transferidos para os EUA por empresas certificadas participantes no sistema de «porto seguro» levanta novas questões graves sobre a continuidade dos direitos dos cidadãos europeus em matéria de proteção de dados quando os seus dados pessoais são transferidos para os EUA."

O TJUE assinala, na senda da citada Comunicação que as autoridades americanas podiam aceder aos dados pessoais transferidos dos Estados-Membros para os Estados Unidos e tratá-los de um modo incompatível, nomeadamente, com as finalidades da sua transferência, para além do que era estritamente necessário e proporcionado à proteção da segurança nacional (90).

Assim, na análise que é feita da Decisão *Safe Harbor*, o TJUE sublinha que a Comissão não identificou os Estados Unidos como Estado apto a assegurar eficazmente

[474] Disponível em: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_pt.pdf

o nível de proteção adequada exigido pela legislação europeia. Com nesta "omissão" o TJUE determina a invalidade do artigo 1.º da Decisão *Safe Harbor* por violação do artigo 25.º, n.º 6 da Diretiva 95/46/CE interpretado à face da CDFUE (97 e 98)

5.2. Na linha dos Processos C-293/12 e C-594/12, de 8 de abril de 2014 (*Digital Rights Ireland*), o TJUE – relativamente à Diretiva 2006/24/CE com incidência na conservação de dados resultantes de comunicações eletrónicas – entendeu que a diretiva implicava uma ingerência excessiva na vida privada e na proteção de dados por não existir um enquadramento preciso que demonstra-se a sua limitação ao estritamente necessário, violando-se, desta forma o princípio da proporcionalidade nas suas várias vertentes (65). Em conformidade com a jurisprudência anterior o TJUE considerou que (93):

> " (…) não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União para os Estados Unidos sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam."

De facto, a Decisão *Safe Harbor*, no artigo 3.º, n.º 1 determinava que:

> "Sem prejuízo da competência para tomar medidas que garantam o cumprimento das disposições nacionais adotadas por força de outras disposições além das previstas no artigo 25.º da Diretiva 95/46/CE, as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios aplicados em conformidade com as FAQ, se isso se verificar necessário à proteção das pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos seguintes (...)"

Tal significa que esta disposição privava as autoridades nacionais de controlo do exercício dos poderes que eram conferidos pelo artigo 28.º da Diretiva 95/46/UE (102),

conduzindo à conclusão de que a Decisão *Safe Harbor* era inválida por impedir que, em face de uma queixa, as autoridades nacionais de controlo avaliassem umas normas constantes de uma decisão que considerasse garantido um nível de proteção adequado na transferência de dados para um Estado terceiro.

Considerando inválidos os artigo 1.º e 3.º da Decisão *Safe Harbor*, o TJUE considerou que, por razões de indissociabilidade, igualmente inválidos os artigos 2.º e 4.º da Decisão.

6. O Processo C-311/18, de 15 de julho de 2020 (*Schrems II*), baseia-se faticamente numa queixa apresentada por Maximilliam Schrems, em 2013, ao DPC irlandês para que suspendesse ou proibisse a transferência dos seus dados pessoais para os EUA, da Facebook Ireland para a Facebook Inc. (77). A queixa foi arquivada com base na existência da Decisão *Safe Harbor* através da qual a Comissão considerava que os Estados Unidos garantiam um nível de proteção adequada de dados pessoais (52).

O requerente apresentou recurso do despacho de arquivamento para o Tribunal Superior da Irlanda, que o invalidou, e que procedeu ao reenvio para o TJUE para que este apreciasse a validade da Decisão *Safe Harbor* (53).

A decisão do TJUE no sentido da invalidade da Decisão *Safe Harbor*, levou a que o Tribunal Superior da Irlanda reformulasse a sua queixa, que levou o requerente a questionar as SCCs (54), por considerar que o Direito norte-americano impunha aos dados provenientes da UE a intervenção da NSA, do *Federal Bureau of Investigation* (FBI) e de diferenciados programas de vigilância, de forma incompatível com os artigos 7.ª, 8.º e 47.º da CDFUE e da legislação europeia de proteção de dados (55).
Posteriormente, o Tribunal Superior incluiu no reenvio questões sobre a validade da Decisão *Privacy Shield* (58).

6.1. O TJUE apreciou a aplicabilidade do RGPD a transferências de dados pessoais para Estados terceiros examinando as exceções constantes do artigo 2.º.
Em decisão, o TJUE afirmou que o Regulamento deve ser interpretado no sentido de a transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num Estado membro para outro operador económico estabelecido em Estado terceiro, para fins de segurança pública, de defesa e de segurança do Estado.

O TJUE considerou que se tratava de uma transferência de dados pessoais entre pessoas coletivas, não se aplicando nenhuma das alíneas do artigo 2.º. (85)[475].

6.2. O órgão de reenvio indagou junto do TJUE qual o nível de proteção exigido pelos artigos 46.º, números 1 e 2, alínea c), do RGPD no âmbito de uma transferência de dados pessoais para um Estado terceiro com base nas cláusulas-tipo de proteção de dados (90). A este respeito compete invocar o considerando 104:

> "Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais setores específicos (…)."

Em decisão, o TJUE afirmou que as duas disposições devem ser interpretados no sentido de que as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes devem assegurar que os direitos dos titulares cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União Europeia pelo RGPD interpretado à luz da CDFUE. Para este efeito, a avaliação do nível de proteção assegurado no contexto dessa transferência deve, nomeadamente, ter em

[475] Ver anotação de Alexandre Sousa Pinheiro ao artigo 2.º in Alexandre Sousa Pinheiro (coordenador), Cristina Pimenta Coelho, Tatiana Duarte, Carlos Jorge Gonçalves e Catarina Pina Gonçalves, "Comentário ao Regulamento Geral de Proteção de Dados", cit., pp. 100 e ss.

consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União Europeia e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no artigo 45.º, n.º 2, do RGPD.

Esta decisão vem na linha de *Schrems I* e assinala a necessidade de aferir a adequação do nível de proteção em todas as fases da transferência de dados, considerando sempre as três alíneas do artigo 45.º, n.º 2.

.

6.3. O órgão de reenvio questiona o TJUE sobre se o artigo 58.º, n.º 2, alíneas f) e j), do RGPD deve ser interpretado no sentido de a autoridade de controlo competente ser obrigada a suspender ou a proibir uma transferência de dados pessoais para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro (106).

Em sede de decisão, o TJUE, na sequência de *Schrems I*, considerou que o artigo 58.º, n.º 2, alíneas f) e j), do RGPD deve ser interpretado no sentido de a autoridade de controlo competente estar obrigada a suspender ou a proibir uma transferência de dados para um Estado terceiro, com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se considerar que essas cláusulas não são ou não podem ser respeitadas pelo Estado em causa, em particular se não existirem condições para cumprir os artigos 45.º e 46.º do RGPD interpretados à face da CDFUE.

6.4. O órgão de reenvio questiona, também, o TJUE, em substância, sobre a validade da Decisão 2010/87/UE da Comissão à luz dos artigos 7.º, 8.º e 47.º da CDFUE (122).
É assinalado que embora as cláusulas sejam vinculativas para o responsável pelo tratamento estabelecido na UE e para o destinatário da transferência de dados pessoais estabelecido num Estado terceiro, o conteúdo do contrato não vincula as autoridades Estado terceiro, por estas não serem partes no contrato (125).

Importa precisar que as decisões de adequação adotadas ao abrigo do artigo 45.º, n.º 3 do RGPD implicam um exame pela Comissão da regulamentação de um Estado terceiro à face, por exemplo, da legislação pertinente em matéria de segurança nacional e

de acesso das autoridades públicas aos dados pessoais e ao acesso das autoridades públicas do Estado terceiro a esses dados (129).

Na ausência de decisão de adequação tomada pela Comissão, o artigo 46.º, n.º 1, do RGPD prevê que os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (128).

A natureza contratual – logo não absoluta - das cláusulas-tipo aprovadas pela Comissão ao abrigo do artigo 46.º, n.º 2, alínea c) do RGPD pode fazer com que responsáveis ou subcontratantes necessitem, em função da situação existente em determinado Estado terceiro, da adoção de medidas suplementares para assegurar o respeito desse nível de proteção (133).

A análise que o TJUE fez das cláusulas da Decisão 2010/87/UE da Comissão, de 5 de fevereiro foram no sentido de considerar que se encontram aptas a garantir transferências de dados com respeito pelo RGPD e para Estados ou territórios onde exista cumprimento da legislação europeia de proteção de dados. Pode haver necessidade de adotar medidas adicionais, mas nesse caso está-se perante uma responsabilização do responsável pelo tratamento ou do seu subcontratante estabelecidos na União e, subsidiariamente, da autoridade de controlo competente (134).

Em sede de decisão, o TJUE entendeu que: "a Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016, à luz dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais não revelou nenhum elemento suscetível de afetar a validade desta decisão."

6.5. O órgão de reenvio questiona se o Direito norte-americano assegura o nível de proteção adequada exigido pelo Direito da UE, podendo questionar-se, assim, a validade da Decisão *Privacy Shield* (168). O TJUE faz uma apreciação sobre a direito à vida privada e o direito à proteção de dados, bem como as condições que habilitam as suas derrogações, obedecendo ao princípio da proporcionalidade, segundo as quais devem ocorrer na estrita medida do necessário, prever regras claras e precisas que regulem o alcance da restrição e os requisitos mínimos, de modo que as pessoas cujos dados foram

transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. A necessidade de dispor destas garantias releva quando os dados pessoais são sujeitos a um tratamento automatizado (176).

Relativamente ao impacto que a legislação norte-americana apresenta nos dados pessoais transferidos da UE, o TJUE afirma, na linha das conclusões do Advogado-Geral, que os programas de vigilância baseados na secção 702 da FISA não são suscetível de assegurar um nível de proteção substancialmente equivalente ao garantido pela CDFUE, conforme interpretada pela jurisprudência do TJUE (179 e 180).

Ainda que a Decisão *Privacy Shield* preveja que a secção 702 da FISA observe os requisitos da Presidential Policy Directive 28 (PPD-28), o TJUE menciona que solicitado a esclarecer o Executivo norte-americano informou que a PPD-28 não confere aos titulares dos dados direitos oponíveis às autoridades americanas nos tribunais (181), apesar de e na Decisão *Privacy Shield* se afirmar que (69):

> "A *Presidential Policy Directive* 28 («PPD-28»), emitida em 17 de janeiro de 2014, impõe várias limitações às operações de «informação de origem eletromagnética». Esta PPD é vinculativa para os serviços de informações norte-americanos e permanece em vigor após a alteração da administração dos EUA. A PPD-28 é de especial importância para os cidadãos de países terceiros, nomeadamente para os titulares de dados da UE."

Quanto aos programas de vigilância baseados na Executive Order 12333--United States intelligence activities (E.O. 12333), decorre dos autos que esse decreto também não confere direitos oponíveis às autoridades americanas nos tribunais (182).

Neste quadro normativo, não existem requisitos de equivalência substancial com o previsto no Direito da UE, particularmente com os artigos 47.º e 52.º, n.º 1, da CDFUE. O TJUE, em consequência do que assinala, considera que a regulamentação enunciada não prevê nenhuma possibilidade de o particular recorrer a medidas jurídicas corretivas eficazes para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva (187).

Relativamente à figura do mediador (*ombudsman*) previsto na Decisão *Privacy Shield*, o TJUE adverte para que se trata de uma figura sem autonomia para a proteção de direitos de titulares de dados oriundos da UE (195):

"O Mediador para o *Privacy Shield* embora descrito como sendo «independente do setor das informações», foi apresentado como «[respondendo] diretamente perante o Secretário de Estado, que assegurará que este desempenhe as suas funções de forma objetiva e isenta de influências indevidas que possam afetar a resposta a fornecer». Por outro lado, além do facto de, como a Comissão constatou no considerando 116 dessa decisão, o Mediador ser nomeado pelo Secretário de Estado e fazer parte integrante do Departamento de Estado dos Estados Unidos, não existe, na referida decisão, como salientou o Advogado-Geral no n.º 337 das suas conclusões, nenhuma indicação de que a destituição do Mediador ou a anulação da sua nomeação sejam acompanhadas de garantias especiais, o que pode pôr em causa a independência do Mediador relativamente ao poder executivo."

Neste contexto, a Decisão *Privacy Shield* foi considerada inválida, com produção imediata de efeitos.

De acordo com o TJUE não se verificaria vazio jurídico dada a aplicação das SCCs e das derrogações constantes do artigo 49.º do RGPD.

6.6. Apesar da afirmação do TJUE vive-se claramente num clima de incerteza na aplicação do Direito da União Europeia no que toca à transferência de dados para Estados terceiros, particularmente para os Estados Unidos.

De salientar que existem posições importantes sobre o futuro *pós Privacy Shield*:

(a) Comité Europeu de Proteção de Dados: *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems.* Adotadas a 23 de julho de 2020;

(b) Comité Europeu de Proteção de Dados*: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. Adotadas a 10 de novembro de 2020;

(c) Comité Europeu de Proteção de Dados; *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures,* adotadas a 10 de novembro de 2020.

—

Acórdão do Tribunal de Justiça (Grande Secção) de 17 de Dezembro de 2020

Comissão Europeia/Hungria

(Processo C-808/18)

(«Incumprimento de Estado — Espaço de liberdade, segurança e justiça — Políticas relativas aos controlos nas fronteiras, ao asilo e à imigração — Diretivas 2008/115/CE, 2013/32/UE e 2013/33/UE — Procedimento de concessão de proteção internacional — Acesso efetivo — Procedimento na fronteira — Garantias processuais — Colocação obrigatória em zonas de trânsito — Detenção — Regresso dos nacionais de países terceiros em situação irregular — Recursos interpostos das decisões administrativas de indeferimento do pedido de proteção internacional — Direito de permanecer no território»)

PARTES

Demandante: Comissão Europeia (representantes: M. Condou-Durande, A. Tokár e J. Tomkin, agentes) *Demandada*: Hungria (representantes: M.Z. Fehér e M. M. Tátrai, agentes)

A Hungria não cumpriu as obrigações que lhe incumbem por força do artigo 5.º, do artigo 6.º, n.º 1, do artigo 12.º, n.º 1, e do artigo 13.º, n.º 1, da Diretiva 2008/115/CE do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativa a normas e procedimentos comuns nos Estados-Membros para o regresso de nacionais de países terceiros em situação irregular, do artigo 6.º, do artigo 24.º, n.º 3, do artigo 43.º e do artigo 46.º, n.º 5, da Diretiva 2013/32/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional, e dos artigos 8.º, 9.º e 11.º da Diretiva 2013/33/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que estabelece normas em matéria de acolhimento dos requerentes de proteção internacional:

— ao prever que os pedidos de proteção internacional apresentados por nacionais de países terceiros ou apátridas que, vindos da Sérvia, pretendam aceder, no seu território, ao procedimento de proteção internacional, apenas podem ser apresentados nas zonas de trânsito de Röszke e de Tompa, adotando ao mesmo tempo uma prática administrativa constante e generalizada que limita drasticamente o número de requerentes autorizados a entrar diariamente nessas zonas de trânsito;

— ao instituir um sistema de detenção generalizada dos requerentes de proteção internacional nas zonas de trânsito de Röszke e de Tompa, sem respeitar as garantias previstas no artigo 24.º, n.º 3, e no artigo 43.º da Diretiva 2013/32, bem como nos artigos 8.º, 9.º e 11.º da Diretiva 2013/33;

— ao permitir o afastamento de todos os nacionais de países terceiros em situação irregular no seu território, com exceção daqueles que são suspeitos de terem cometido uma infração, sem respeitar os procedimentos e garantias previstos no artigo 5.º, no artigo 6.º, n.º 1, no artigo 12.º, n.º 1, e no artigo 13.º, n.º 1, da Diretiva 2008/115;

— ao sujeitar as condições contrárias ao direito da União o exercício, pelos requerentes de proteção internacional abrangidos pelo âmbito de aplicação do artigo 46.º, n.º 5, da Diretiva 2013/32, do seu direito de permanecer no seu território.

COMENTÁRIO

Elizabeth Accioly[476]

O acórdão do Tribunal de Justiça da União Europeia (TJUE), de 17 de dezembro de 2020, foi publicado no Jornal Oficial da União Europeia de 15.2.2021 PT (C 53/3). Trata-se de uma ação por incumprimento, prevista nos artigos 258º a 260º do Tratado sobre o Funcionamento da União Europeia (TFUE), que tem por demandante a Comissão Europeia e por demandada a Hungria, quanto ao desrespeito da legislação derivada da União Europeia sobre a politica migratória e de refúgio, (Diretivas 2008/115, 2013/32 e 2013/33), bem como à Carta de Direitos Fundamentais da União

[476] Doutora em Direito Internacional pela Universidade de São Paulo-USP. Diplomada em Estudos Europeus pela Universidade de Lisboa. Advogada, inscrita na Ordem dos Advogados de Portugal e do Brasil. Professora Auxiliar da Universidade Europeia de Lisboa. Professora Visitante do Programa de Mestrado e Doutoramento do Centro Universitário de Curitiba-Unicuritiba-Brasil. Colaboradora do Instituto Europeu da Faculdade de Direito de Lisboa. Leciona as disciplinas de Direito da União Europeia, Direito Internacional Público, Contencioso da União e Direito da Integração Latino Americana. Autora das obras: "Mercosul e União Europeia", 4ª ed., editora Juruá-Brasil; "Sistema de Solução de Controvérsias em Blocos Económicos", Ed. Almedina-Lisboa; ”Direito no Século XXI", Editora Juruá-Brasil, e de vários artigos publicados em obras coletivas e revistas jurídicas, nacionais e internacionais. Membro da Academia Paranaense de Letras Jurídicas. Membro da Academia de Cultura de Curitiba – ACCUR. Membro do Instituto dos Advogados do Paraná, Membro Fundador da *European Community Studies Association América Latina* - ECSA-AL e da *European Community Studies Association* - ECSA-Brasil. Condecoração Medalha do Mérito Rosalba, conferido pelo Tribunal Permanente de Revisão do Mercosul.

Europeia (CDFUE) e ao Direito Internacional Público e à Convenção Europeia de Direitos Humanos.

A Hungria tornou-se membro da União Europeia em 1.05.2004, no maior alargamento de sempre, ao lado de outros nove Estados (Estónia, Letónia, Lituânia, Eslováquia, Eslovênia, Polónia, República Checa, Malta e Chipre). Naquela altura de 15 a Europa passou a funcionar a 25; depois a 28, com a entrada da Roménia e da Bulgária, em 2007, e finalmente da Croácia em 2013. Atualmente, com a saída do Reino Unido, em 31.01.2020, a UE possui 27 Estados membros.

Todos os Estados que aderem ao bloco económico devem respeitar as normas da União Europeia, seja de direito originário ou de direito derivado, amparado pelo princípio do primado do Direito da União Europeia sobre o direito interno, que diferencia a União Europeia dos demais blocos económicos que foram criados, pelo seu caráter supranacional, cerne do edifício comunitário, desde os seus primórdios, em 1957. Incumbe aos Estados que a este bloco se associam cumprir o que foi convencionado não nos seus tratados institutivos, mais respeitando também um dos princípios basilares do Direito Internacional – a *pacta sunt servanda*. No entanto, os Tratados preveem punição aos Estados, em caso de não cumprimento das normas comunitárias, com a atuação de um de seus órgãos, que tem a missão de ser o guardião do respeito das normas comunitárias: o Tribunal de Justiça da União Europeia (TFUE).

Vários são os recursos cabíveis ao TJUE, elencados nos artigos 258º a 279º do TFUE. O acórdão que ora se analisa trata de uma ação por incumprimento, prevista nos artigos 258º a 260º, ação de competência exclusiva do TJUE, com a supressão do Tribunal Geral, outrora Tribunal de 1ª Instância. Neste caso, os Estados infratores são levados perante o TJUE, quando estiver em causa o desrespeito ao arcabouço comunitário. Há, porém, uma fase pré-contenciosa, com a intervenção da Comissão, que atua como mediador para repor o cumprimento da norma comunitária – originária ou derivada, sem a necessidade de o Estado ser levado ao TJUE. Somente quando esta etapa não é frutífera, a Comissão, após emitir um parecer fundamentado sobre o caso, submete-o ao TJUE.

No presente acórdão foi emanado pelos juízes do TJUE, em 17 de dezembro de 2020 e publicado no Jornal Oficial da UE (C 53/3 – de 15.02.2021). Antes disso, porém, uma tentativa pré-contenciosa já se arrastava desde 2015, no auge da crise dos refugiados, quando a EU, deparou-se com a posição pouco recetiva de alguns Estados membros,

quanto à aceitação de milhares de refugiados e migrantes que desembarcavam no velho continente, em busca de uma vida digna, a invocar o estatuto de refugiado ou de migrante económico. Dentre eles, a Hungria resistia às normas vindas de Bruxelas, construindo muros verdadeiros, com a vizinha Sérvia, para vedar a entrada daqueles que por ali chegavam, mas também muros legislativos, com a aprovação de leis internas que afastavam *tout court* aqueles que insistiam em forçar a sua entrada em território húngaro.

O procedimento pré-contencioso teve início em dezembro de 2015, quando a Comissão enviou à Hungria uma notificação, acusando aquele Estado de ter violado, designadamente, o artigo 46.º, n.os 1, 5 e 6, da Diretiva 2013/32, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional e da Diretiva 2013/33, que estabelece normas em matéria de acolhimento dos requerentes de proteção internacional. A Hungria alegou, em sua resposta, que a sua regulamentação interna era compatível com o direito da União.

Passado pouco mais de um ano, em março de 2017, o parlamento húngaro aprovou uma lei que permite a detenção automática de todos os migrantes em busca de asilo no país, desde que não apresentem a documentação necessária para a sua concessão, sendo detidos em campos nas fronteiras ao sul – em especial com a Sérvia – e impedidos de circular livremente. A Comissão, uma vez mais, volta a interpelar a Hungria, considerando que a lei recém-aprovada era suscetível de suscitar preocupações suplementares às que já tinham sido expostas. No dia 18 de maio do mesmo ano, a Comissão enviou outra notificação, agora por não respeitar, para além das Diretivas acima citadas, a Diretiva 2008/115, relativa a normas e procedimentos comuns nos Estados-Membros para o regresso de nacionais de países terceiros em situação irregular. Em 18 de julho de 2017 a Hungria responde à notificação complementar da Comissão, afirmando que a lei em questão era compatível com o direito da União. No dia 8 de dezembro de 2017, a Hungria foi notificada, através de um parecer fundamentado da Comissão, do não cumprimento das diretivas supramencionadas, conjugados com os artigos 6.º, 18.º e 47.º da Carta de Direitos Fundamentais da União Europeia, parecer que foi encaminhado ao TJUE, encerrando assim, sem sucesso, a fase pré-contenciosa.

O TJUE declarou, no acórdão proferido em dezembro de 2020, que a Hungria não está a cumprir as obrigações que lhe incumbem, enquanto Estado membro da UE, no que diz respeito à garantia de proteção internacional aos requerentes de asilo, estabelecidas nas

diretivas 2008/115, 2013/32 e 2013/33. Ficaram comprovados reenvios ilegais de refugiados – nomeadamente na fronteira servo-húngara, considerados uma afronta não só ao Direito da União Europeia como também ao Direito Internacional e aos Direitos Humanos. A Hungria é o único Estado membro da UE a ter a prática de "pushbacks" prevista na sua legislação interna, prática esta que viola o direito derivado europeu (Diretivas 2008/115; 2013/32 e 2013/33) e a Carta dos Direitos Fundamentais da União Europeia, bem como várias leis internacionais, dentre elas o Estatuto dos Refugiados e a Convenção Europeia dos Direitos Humanos.

O Estatuto dos Refugiados foi formalmente adotado em 28 de julho de 1951, com o intuito de estabelecer normas para os refugiados no período pós-guerra. Para tanto, foi criado o Alto Comissariado das Nações Unidas para os Refugiados – ACNUR, que tem por finalidade definir quem pode invocar o estatuto de refugiado e esclarecer os seus direitos e deveres nos países onde são acolhidos, e zelar pelo cumprimento das suas normas. É de todo oportuno invocar o art. 33º do Estatuto, para confrontar a reprovável atitude húngara, que aliás, deve respeito a esta lei internacional, por ser signatária do Estatuto, desde 1989: *"nenhum dos Estados Contratantes expulsará ou repelirá um refugiado, seja de que maneira for, para as fronteiras dos territórios onde a sua vida ou a sua liberdade sejam ameaçadas em virtude da sua raça, religião, nacionalidade, filiação em certo grupo social ou opiniões políticas."*

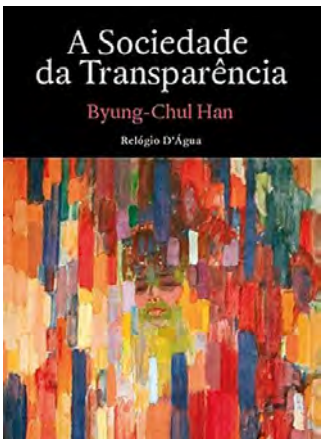
A proibição de expulsões coletivas de estrangeiros está prevista no Protocolo 4 da Convenção Europeia de Direitos Humanos, de 16.09-1963. Constata-se aqui outro desrespeito flagrante do Direito Internacional, por ter a Hungria ratificado a CEDH no ano de 1992. E, na esteira da proteção dos Direitos Humanos, a Hungria afronta, enquanto membro da UE desde 2004, a Carta dos Direitos Fundamentais da União Europeia, especificamente o artigo 6.º, quanto ao direito à liberdade e à segurança; o artigo 18.º que garante o direito ao asilo, no quadro do Estatuto dos Refugiados, de 1951 e nas normas estabelecidas nos seus Tratados institutivos; e o artigo 47.º, que confere a toda pessoa cujos direitos e liberdades garantidos pelo direito da União tenham sido violados, o direito a uma ação perante um tribunal imparcial.

Por outro lado, as OnG são atores importantes na sociedade internacional, pese embora não tenham adquirido o estatuto de sujeito de direito internacional, mas que, sem dúvida, contribuem, através de protestos e denúncias, trazendo ao conhecimento do público casos

de afronta aos direitos humanos, ao meio ambiente, entre outros temas igualmente relevantes. No caso que ora se comenta, a *Hungarian Helsinki Committee*, a *Human Rights Watch* e os Médicos Sem Fronteiras têm denunciado a prática recorrente de "pushbacks" na Hungria e, mais recentemente, na fronteira entre a Grécia e a Turquia, manchando a reputação da União Europeia no que diz respeito à política de migração e asilo ao apontar o dedo para uma das suas agências - a Agência Europeia de Guarda Costeira e de Fronteiras – FRONTEX, que tem por missão patrulhar as fronteiras externas da UE. Recai sobre esta agência a acusação de fechar os olhos aos reenvios ilegais e de ser conivente com a Hungria e a Grécia, onde tem postos de patrulhamento.

Diante de tais factos, e na esteira do acórdão do TJUE que aqui nos debruçamos, a FRONTEX suspendeu, no início de 2021, as suas operações na Hungria, justamente para tentar ilibar-se das acusações que tem sido alvo. Numa altura em que a União Europeia discute a reforma da **política** migratória e de asilo, com o anúncio de um novo Pacto para as Migrações, é fundamental uma posição mais firme e rápida nos casos como o do presente acórdão, com Estados a desrespeitar os Direitos Humanos, o Direito Internacional, o Direito da União Europeia, em especial, os valores elencados no artigo 2º do Tratado da União Europeia. Também é urgente resgatar o prestígio da FRONTEX que tem a função de zelar pelas fronteiras que emolduram a muralha europeia, mas nunca a de compactuar com Estados incumpridores.

IV_Recensões



A Sociedade da Transparência

Byung-Chul Han
Relógio de Água, 2014

José Conde Rodrigues

Neste mundo desapiedado e devassado não há mais lugar para o sofrimento íntimo, recolhido, que os bichos ainda podem sentir na toca. Agora já ninguém é dono de si e dos seus segredos. Somos públicos e baldios.

Miguel Torga, Diários, XVI

O uso da informação, a luta pelos dados, quem os domina, quem os tem seguros, quem os rouba, quem os manipula, como se garante a sua privacidade, como são usados e partilhados, para fins económicos ou securitários, define a natureza e os termos da nova conflitualidade à escala planetária, o novo âmbito do potencial conflito entre as potências incumbentes e emergentes[478].

Neste confronto, que espelha a nossa historicidade, está em causa também a relação entre o humano e a técnica, os desafios enfrentados pelo tempo e a beleza, mas, sobretudo, a defesa da intimidade, da proximidade e da alteridade, numa sociedade cada vez mais em rede[479], obcecada com a transparência e o consumo volátil, transformada num verdadeiro enxame digital e dominada pela psicopolítica.

Sobre todos estes temas se tem pronunciado Byung-Chul Han, autor de origem coreana, a investigar e a exercer a docência na Alemanha, desde os anos oitenta do século passado.

É sobre a sua obra, *A Sociedade da Transparência*, publicada na Alemanha em 2012, mas cuja atualidade é manifesta, que assenta esta pequena recensão. Segundo o

[478] Para ajudar nesta leitura da atual realidade política internacional, ver com muito interesse, Niall Ferguson, ***A Praça e a Torre – Redes, Hierarquias e a Luta pelo Poder Global***, Lisboa: Temas & debates, 2018.

[479] Ver sobre este conceito, a obra seminal de Manuel Castells, ***A Sociedade em Rede***, vol. 1, 3º ed., S. Paulo: Paz e Terra, 2000.

autor, *nenhum outro tema, no discurso público, é hoje tão dominante como o da transparência*.

Mas o tema também se liga com os novos movimentos sociais em rede digital, com a criação de sites de revelação de *segredos*, com a pretensa luta contra a corrupção ou com e a defesa das liberdades, nomeadamente de expressão ou religião.

Para o filósofo germano-coreano, as coisas tornam-se transparentes quando se despojam da sua singularidade[480], constituindo a sociedade da transparência um verdadeiro inferno igualitário. Acrescentando mesmo que *só a máquina é transparente. A espontaneidade, o que é do registo de um acontecer e a liberdade, traços que constituem a vida em geral, nada comportam de transparência*. E acrescenta ainda o autor que, *sabendo o que fazemos, contribuímos para o panótico digital, na medida em que nos desnudamos e nos expomos.*

Vivemos, assim, envolvidos por um grande panótico digital, onde todos se sujeitam voluntariamente à transparência. A vigilância e o controlo não surgem como ataques à liberdade, pois, ao exporem a sua vida, os seus gestos, os seus sentimentos, o seu corpo, os seus negócios, todos se entregam a todos. Sem o segredo inerente à reserva da viva privada, centro da intimidade numa digna vida humana, todos se expõem ao grande irmão, ao olhar central das grandes empresas de comunicações e plataforma de gestão de dados, bem como aos Estados, mais ou menos autoritários, e usam as suas tecnologias. É que, muitas vezes, a falta de distância, cega-nos, e a transparência não equivale à verdade. E numa altura em todos passámos a usar máscara, também não pode ter o significado de desvelar ou desmascarar, como se vivêssemos num mundo imerso na suspeita permanente.

A ligação direta do cidadão/consumidor com as grandes empresas e o Estado, sem intervenção das tradicionais estruturas intermédias da sociedade civil também aponta para um novo totalitarismo digital que, sem controlo político democrático, vai enfraquecendo a liberdade individual e a responsabilidade pessoal, destruindo a coesão social, em nome muitas vezes de mais rapidez, mais proximidade, mais e mais transparência.

[480] Singularidade que significa também o momento em que a máquina se funde com o humano, na evolução da nova inteligência artificial, cf. Jean Gabriel Ganascia, ***O Mito da Singularidade***, Lisboa: Temas & Debates, 2018; ou ainda, Pedro Domingos, ***A Revolução do Algoritmo Mestre***, Lisboa: Manuscrito, 2017.

No fundo, a revolução digital, a terceira revolução industrial[481] a nova era digital[482], a Internet e as redes sociais, estão a transformar o mundo e as sociedades em que vivemos.

Neste livro, Byung-Chul Han afirma que a atual obsessão com a transparência se manifesta, sobretudo, porque a confiança desapareceu e a sociedade aposta cada vez mais na vigilância[483] e no controlo.

Segundo o filósofo germano-coreano, a sociedade da transparência é o inferno do igual, isto é, numa sociedade imersa na transparência não existe verdadeiro sentido comunitário, mas a apenas a acumulação de indivíduos incapazes de uma ação cívica conjunta.

No fundo, a vontade de vigiar e ser vigiado acaba por parecer algo natural e voluntário, qual ato de aparente liberdade, pois cada qual se lhe entrega voluntariamente, expondo-se ao olhar global, panótico, que transforma cada ser humano, simultaneamente, em vítima e agressor.

A somar a este estado de coisas devemos, ainda segundo o nosso autor, juntar o panorama da comunicação e da informação, que tudo parece querer penetrar e tudo transforma em vazio, em instantâneo, em não lugar. Estamos perante uma espécie de vento digital que sopra através da sociedade da transparência. As redes sociais, por exemplo, são apenas aparentemente transparentes, pois são as mesmas que filtram conteúdos, que induzem informações subliminares para consumo ou que criam desinformação política e social em muitos regimes autoritários por esse mundo fora. Não estão submetidas a qualquer imperativo moral e são, no fundo, desprovidas de qualquer virtual ou remoto superego.

A situação agrava-se mais se pensarmos no poder inerente aos diferentes motores de busca, às diversas plataformas de interação social que, apresentando-se como espaços de liberdade, tendem, afinal, a converter-se num olho gigante, quase infinito, de onde tudo se observa e comenta. E o mais impressivo é que, ao contrário das soluções distópicas e concentracionárias imaginadas por Orwell ou Huxley, nestes novos espaços

[481] Sobre o modo como a nova era da informação está a mudar a energia, a economia e o mundo, cf. Jeremy Rifkin, ***A Terceira Revolução Industrial***, Lisboa: Bertrand Editora, 2014.
[482] Acerca do impacto da digitalização no futuro das pessoas, das nações e da economia, cf. Eric Schmidt/Jared Cohen, ***A Nova Era Digital***, Lisboa: 2013.
[483] Refletindo sobre o impacto da vigilância na moderna economia, cf. Shoshana Zuboff, ***A Era do Capitalismo da Vigilância***, Lisboa: Relógio de Água, 2020.

públicos, ninguém impõe a transparência, pelo contrário, somos nós que nos sujeitamos alegre e voluntariamente ao seu reino omnipresente.

Vivemos assim voluntariamente submetidos à referida obsessão com a transparência. Toda a gente clama por mais transparência. Por uma política transparente, por uma economia transparente, mas, mais do que isso, por uma vida privada e mesmo íntima, transparente. Sem paredes, sem vidros, sem cortinas: a abertura total. A sociedade transparente. O verdadeiro desvelamento do ente, que assim se abre ao ser, para usar uma expressão cara a Heidegger.

A vida humana, porém, construiu-se sempre num trágico equilíbrio entre o segredo e a revelação. A humanidade é privacidade. Todos nós necessitamos de um espaço e de um tempo só nosso, qual grande reduto da nossa liberdade interior. Esse espaço é, noutras palavras, o núcleo do nosso mínimo ético. O centro onde se cruzam a nossa essência e a nossa existência. O ponto de Arquimedes da dignidade humana. A natureza, essa sim, é nua, aberta, transparente. Exigir, reclamar, pois, a transparência total, é defender o fim do humano e do seu mistério.

Reconhece-se que manter esse equilíbrio é cada vez mais uma tarefa difícil e inglória. Cada vez é mais difícil guardar algum espaço humano livre do olhar ou do ouvido do outro. É cada vez mais difícil o balanço entre, por um lado, a defesa da intimidade, a defesa do indivíduo e da sua circunstância pessoal e, por outro, o interesse público que exige o pleno respeito pelo princípio jurídico-público da transparência. Ou seja, o tema da transparência, não só veio para ficar como se tornou dominante no espaço público.

Dito isto, tal não significa que o autor defenda, nesta sua obra sobre a transparência, qualquer intransigente opacidade ou o segredo como modo de vida social ou pública, antes pretende apresentar-se como um alerta para o perigo do discurso aparentemente sedutor da híper-transparência nas sociedades contemporâneas.

Uma coisa é ser a favor da máxima transparência na defesa do interesse público, bem como do uso intransigente da responsabilização política e ética inerente a um verdadeiro Estado de Direito, outra coisa é a demagogia associada à transparência que impera no atual espaço público e, infelizmente, também cada vez mais no espaço privado.

É que, paradoxalmente, ao mesmo tempo em que se exortam as maravilhas da transparência, em que proliferam os programas televisivos das casas sem segredos, e assistimos ao sucesso planetário (infelizmente fogaz) do *Wikileaks* e dos *Panama Papers*

ou Footballeaks, assiste-se também ao regresso das fronteiras, ao retorno dos muros, à exclusão, ao nacionalismo xenófobo e radical.

Convém não esquecer que os regimes totalitários sempre exigiram a total transparência na vida dos seus súbditos. Nesses regimes, o recurso ao discurso da transparência significou e, infelizmente, ainda significa, a via aberta para a opressão, o domínio ilegítimo, o controlo irrazoável, numa palavra, a supressão total da liberdade. Como se todos soubessem tudo sobre todos, mas em que alguém, sabendo mais, usa esse conhecimento para edificar um mundo concentracionário, através do qual domina os outros.

E preocupante é ainda o facto de o autor ora em apreço admitir que o atual modo de vida, mesmo em sociedades demoliberais acossadas pelo flagelo do terrorismo que hiperboliza o sentimento de insegurança, acarreta a armadilha da transparência e da informação total. Também aqui, infelizmente, corremos o risco de pôr em causa o nosso espaço vital de liberdade, o reduto íntimo da nossa vivência humana.

Ou seja, quer no reino do sagrado, quer no domínio do estrito viver humano, nunca poderemos saber tudo, nunca poderemos ver ou ouvir tudo. Haverá sempre um encantamento do mundo que surge do mistério. Existirá sempre um caminho de descoberta. No dia em que esse mistério e esse caminho da descoberta desaparecerem, a vida, tal como a conhecemos, deixará de ter sentido.

Em suma, mais que duma sociedade transparente, precisamos, isso sim, de uma sociedade translúcida. Muito, muito, lúcida… Ou, terminando com as palavras de Byung-Chul Han, precisamos, urgentemente, de enfatizar que *"a alma humana tem necessidade de esferas nas quais possa estar em si mesma sem o olhar do outro".*