

# Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 03 – DEZEMBRO 2021

ONLINE

---

## Direção Executiva

Cristina Maria de Gouveia Caldeira  
Alexandre Sousa Pinheiro



Universidade  
Europeia

PRIVACY AND DATA PROTECTION CENTRE



---

# Privacy and Data Protection Magazine

**Data:** dezembro 2021

**Publicações:** 3 números anuais

## 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 Colaboraões.** A Revista publica em acesso aberto artigos doutrinários e outros estudos, legislação e jurisprudência comentadas e resenhas de obras científicas.

**8.º Conselho Editorial.** Após revisão por pares, a seleção dos trabalhos a publicar é feita por um Conselho Editorial integrado 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) Resenhas.

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



**Universidade  
Europeia**

PRIVACY AND DATA PROTECTION CENTRE



# Ficha Técnica

**Título**

Privacy and Data Protection Magazine

**Subtítulo**

Revista Científica na Área Jurídica

**Número**

003

**Ano de Publicação**

2021

**Afiliação**

Privacy and Data Protection Centre – Universidade Europeia

**Conselho Editorial**

Alexandra Chícharo das Neves

Ana Cristina Roque

Eduardo Vera-Cruz

Ingo Wolfgang Sarlet

Luís Filipe Coelho Antunes

Pedro Barbas Homem

**Autores**

Cristina Maria de Gouveia Caldeira

Gabriel Pestana

Joana Capaz Coelho

Lurdes Dias Alves

Maria Cláusia Cachapuz

Maria Luiza Kurban Jobem

Pedro Barbas Homem

Pedro Rebelo Botelho Alfaro Velez

Vera Lúcia Raposo

Sílvia Levenfus

**Prefácio**

Cristina Maria de Gouveia Caldeira

Alexandre Sousa Pinheiro

**Direção Executiva**

Cristina Maria de Gouveia Caldeira

**ISSN**

2184-920X

**Número de Registo**

127600

**Propriedade**

ENSILIS - Educação e Formação, Unipessoal, Lda.

**Chief Executive Officer**

Miguel Carmelo

**NIPC/NIF**

504 669 788

**Editor e Redação**

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



**Universidade  
Europeia**

**PRIVACY AND DATA PROTECTION CENTRE**



# Índice

Prefácio .....	1
<b>I_Artigos Doutrinários .....</b>	<b>4</b>
<b>Acerca da Revista Privacy and Data Protection Magazine .....</b>	<b>5</b>
Pedro Barbas Homem	
<b>Proposta de Regulamento sobre Inteligência Artificial: The devil is in the details .....</b>	<b>9</b>
Vera Lúcia Raposo	
<b>E-Judiciário e automação: freios e avanços na experiência brasileira .....</b>	<b>25</b>
Maria Cláudia Cachapuz, Maria Luiza Kurban, Jobim Silvia Levenfus	
<b>A Proteção da Privacidade dos Denunciantes à luz da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro, relativa à Proteção das Pessoas que denunciem violações do Direito da União .....</b>	<b>47</b>
Joana Capaz Coelho	
<b>O “Espírito Dominicano” no Pensamento Político-Constitucional Occidental: Algumas Notas .....</b>	<b>69</b>
Pedro Rebelo Botelho Alfaro Velez	
<b>II_Outros Estudos.....</b>	<b>82</b>
<b>A evidência digital na cadeia de custódia electrónica para incidentes CBRNE .....</b>	<b>83</b>
<b>III_Legislação e Jurisprudência Comentadas.....</b>	<b>94</b>
<b>Comentário ao Acórdão do Tribunal da Relação de Coimbra relativo ao Processo 302/19.2T8MGL.C1, de 29 de junho de 2021 .....</b>	<b>95</b>
<b>IV_Recensões .....</b>	<b>118</b>
<b>Teoria Geral do Direito Digital: Transformação Digital Desafios para o Direito, Wolfgang Hoffmann-Riem, 2021 .....</b>	<b>119</b>
Cristina Maria de Gouveia Caldeira	

## Prefácio

A revista *Privacy and Data Protection Magazine* encerra o ano de 2021, prosseguindo o seu compromisso de publicação regular, em acesso aberto, com um especial contributo do Professor Doutor Pedro Barbas Homem, que nos recorda o nascimento da revista e a sua relevância científica.

A afirmação cada vez maior da PDPM no panorama internacional, tem atraído investigadores estrangeiros, oriundos principalmente de países de língua oficial portuguesa. Com o objetivo de contribuir para o aprofundamento da doutrina e de outros estudos desenvolvidos no Centro de investigação, o *Privacy and Data Protection Centre*, a Direção Executiva avança no sentido de cumprir novos requisitos, nomeadamente a integração da revista no Portal de Repositórios Científicos de Acesso Aberto em Portugal, administrado pela Fundação para a Ciência e Tecnologia, I.P.

Temáticas como a inteligência artificial, já tratada no número anterior, volta a ser objeto de estudo, num artigo que nos alerta para o entusiasmo em torno da publicação da Proposta de Regulamento sobre a Inteligência Artificial, mas também de alguma desilusão por todos aqueles que consideram que os direitos fundamentais não foram suficientemente acautelados.

A referência à implementação de medidas pelos tribunais brasileiros para a adequação à Lei Geral de Proteção de dados (LGPD), e a alusão à publicação da Resolução n.º 363/2021, de janeiro de 2021, são da autoria de investigadoras que vivenciam na prática, os progressos alcançados no Brasil, em matéria de privacidade e proteção dos dados pessoais. Nessa reflexão, evidencia-se o papel do Encarregado de Proteção de Dados, e de uma Comissão de Estudos criada especificamente para a implementação da LGPD no Tribunal de Justiça do Rio Grande do Sul.

A proteção da privacidade dos denunciantes, é analisada à luz da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro. A autora aborda as garantias de proteção de dados e de confidencialidade das informações obtidas, num contexto onde se procura combater a fraude e a corrupção, tanto no Estado como nas empresas.

As fundações dos direitos humanos são magistralmente tratadas num artigo que versa sobre o significado no e para o pensamento político-constitucional ocidental da teoria político-jurídica produzida no seio da ordem dominicana.

Em sede de “outros estudos” inclui-se um estudo técnico pertinente e atual, que em muito enriquece a abordagem jurídica do tema da autenticidade da prova, já por inúmeras vezes tratada nos debates académicos organizados pelo Centro de Investigação. O autor, que é doutorado na área científica de Sistemas de Informação, apresenta uma abordagem arquitetural assente na especificação de um *workflow* de governação de informação de suporte ao processo de decisão.

Na secção sobre Legislação e Jurisprudência Comentadas, procede-se a um comentário ao Acórdão do Tribunal da Relação de Coimbra relativo ao Processo 302/19.2T8MGL.C1, de 29 de junho de 2021, uma decisão que nos remete para o brocardo “volenti non fit injuria”.

Sendo o Direito do Consumo uma área abrangida pelo objeto da revista, justifica-se uma referência ao Processo C-319/20, para realçar a perspetiva do advogado-geral J. Richard de la Tour, de que os Estados-Membros podem permitir às associações de defesa dos interesses dos consumidores exercer ações coletivas contra



a violação da proteção dos dados pessoais. *Estas ações devem basear-se na violação de direitos que o Regulamento Geral sobre a Proteção de Dados confere aos titulares dos dados*

Por último, apresenta-se a recensão da obra de Hoffmann-Riem, Wolfgang. *Teoria Geral do Direito Digital: Transformação Digital Desafios para o Direito*, Tradução Italo Fuhrmann, Editora Forense, Rio de Janeiro, 2021.

**Cristina Maria de Gouveia Caldeira**





# I\_Artigos Doutrinários

---

# Acerca da Revista *Privacy and Data Protection Magazine*

*Pedro Barbas Homem<sup>1</sup>*

## RESUMO

O lançamento da revista *Privacy and Data Protection* do centro de investigação correspondente da Universidade Europeia corresponde à necessidade de reflexão científica crítica acerca de um tema fundamental dos nossos dias. Mas desde logo se colocam os problemas típicos da ciência do direito acerca da qualificação de um novo ramo do direito e da sua especificidade metodológica, pública ou privada. Certo é que a matéria supera esta divisão e implica a sua complementaridade.

## PALAVRAS-CHAVE

Protecção de dados, ciência jurídica, ramos do direito, licitude

---

<sup>1</sup> Professor Catedrático da Faculdade de Direito da Universidade de Lisboa.

---

# About a new journal on Privacy and Data Protection

*Pedro Barbas Homem<sup>2</sup>*

## ABSTRACT

The launch of the Privacy and Data Protection magazine of the corresponding research center of Universidade Europeia corresponds to the need for critical scientific reflection on a fundamental topic of our times. From the beginning, the typical problems of the science of law arise regarding the qualification of a new branch of law and its methodological specificity, public or private. What is certain is that the subject overcomes this division and implies its complementarity.

## KEYWORDS

data protection, science of law, methodology, lawfulness

---

<sup>2</sup> Professor Catedrático da Faculdade de Direito da Universidade de Lisboa.

Senhora Reitora  
Senhora Professora Cristina Caldeira  
Senhor Professor Alexandre Sousa Pinheiro  
Senhores professores, estudantes e espectadores  
Caros amigos,

É com o maior gosto que me associo a esta sessão de lançamento da revista *Privacy and Data protection Magazine*, revista científica na área jurídica.

Acompanhei os primeiros passos do centro de investigação na matéria da proteção de dados e fico muito feliz por verificar os seus resultados.

A publicação de um jornal científico que obedece às regras da ciência aberta dos nossos dias, nomeadamente quanto à escolha das colaborações, sua revisão científica e indexação mostra que a Universidade Europeia continua a fazer um caminho relevante no domínio da investigação científica.

Não posso deixar de lembrar que a professora Cristina Caldeira foi uma colaboradora de excelência e dedicação aquando do meu exercício de funções diretivas nesta universidade e é uma grande alegria poder revê-la, ainda que à distância.

Excelência e dedicação que ajudam a explicar a publicação que agora temos pela frente, porque o lançamento de uma revista exige um enorme dispêndio de tempo e de energia, que só aqueles que já se dedicaram a estas tarefas conseguem medir e avaliar.

Acerca dos dados informáticos já muito se disse: que são simultaneamente o ouro dos nossos dias, mas que também a maior ameaça aos direitos e liberdades individuais e coletivos.

Que justificam uma nova revolução industrial em curso, eventualmente a quarta, a que se está a seguir uma revolução cultural, cuja extensão ainda não percebemos com clareza, mas que sabemos ter sido potenciada por aquela.

O direito, como é habitual, chega sempre tarde aos acontecimentos.

Como um polícia que é chamada para tomar conta das ocorrências, o direito dos dados concretiza-se frequentemente quando pessoas e empresas já inventaram novas tecnologias e, também frequentemente, os malfeitores inventaram usos e métodos ilegais dos dados.

O direito chega tarde aos acontecimentos, mas chega.

E, com o direito, a reflexão científica.

O direito chega tarde e põe-se a correr para chegar ao seu destino.

O caminho, que pomposamente chamamos metodologia jurídica e metódica da concretização, tem neste plano vários caminhos possíveis e uma extrema perplexidade perante a inventividade da ciência e da tecnologia.

Quanto à ciência e os seus conceitos: o direito relativo aos dados é direito constitucional, público, privado, ou tudo e todos?

A dogmática deste novo ramo do direito tem, efectivamente, que tomar em consideração os Direitos Fundamentais, a Propriedade Intelectual, o Direito do Consumo, o Direito da Saúde, o

Direito Internacional e Europeu, entre outros. Fala-se em Direito Digital e Direito da Inteligência Artificial.

Tomamos consciência dos problemas específicos da proliferação de novos ramos de direito: de um lado, o nascimento de licitudes específicas – e mesmo o campo de um direito administrativo e criminal próprios – com difícil delimitação de fronteiras perante outras licitudes, especialmente as do direito privado, assente na autonomia das pessoas e na heterolimitação pela lei.

Estamos perante uma disciplina cosmopolita porque os problemas são universais, como universais são algumas das soluções: mas tudo o resto permanece, na sua essência, local e da competência de legisladores e tribunais nacionais.

A articulação de planos mostra a difícil metódica de concretização dos planos internacional, regional (sobretudo Conselho da Europa e União Europeia), nacional, institucional (empresas, Estado e instituições públicas) e pessoal.

Como não lembrar a lei da complexidade crescente: como na biologia, uma tendência a um crescimento constante da heterogeneidade e da diversidade, como leis da evolução – se não existirem regras que disciplinem essa evolução.

Somente o aprofundamento científico permite dilucidar estas temáticas e resolver as aporias trazidas pelo progresso da ciência e da tecnologia, estabelecer as fronteiras entre o lícito, o permitido e o proibido e fortalecer as nossas liberdades individuais e colectivas.

Para utilizar uma fórmula de autor, mas hoje consagrada, cabe à ciência do direito diminuir e resolver esta complexidade crescente.

A literatura e as artes trazem todas os dias novas distopias: temos bem consciência de alguns perigos que espreitam, mas, num paradoxo bem próprio da sociedade do conhecimento, estamos dispostos a suportar os riscos desses perigos – porque também estas novas tecnologias ampliam a nossa liberdade e o nosso bem-estar.

É a procura deste equilíbrio que o direito e a sua reflexão científica perseguem e é destes temas que trata a revista científica que hoje lançamos simbolicamente – ela própria e os seus conteúdos já disponíveis no espaço digital.

O Centro de investigação da Universidade Europeia conseguiu nestes tempos de pandemia resultados excelentes, através de webinários e de publicações científicas e, assim, só me resta agradecer a dedicação e o entusiasmo dos seus diretores e formular os votos das maiores felicidades, estando certo de que os merecem.

Parabéns aos diretores, autores e autoridades académicas que tornaram possível a concretização deste projeto de grande qualidade científica.

---

# Proposta de Regulamento sobre Inteligência Artificial: The devil is in the details

Vera Lúcia Raposo<sup>3</sup>

## RESUMO

A recente proposta da Comissão Europeia para um enquadramento jurídico da inteligência artificial na União Europeia – o chamado Regulamento da Inteligência Artificial – foi recebido com entusiasmo, mas também com apreensão e alguma desilusão. Entusiasmo porque um posicionamento legal da União Europeia a este respeito era desde há muito esperado, como forma de impulsionar o projecto digital europeu. Apreensão porque se temem os efeitos da inteligência artificial para os direitos fundamentais dos cidadãos europeus. Desilusão, que é dupla, porque de um lado se alega que os direitos fundamentais não foram acautelados pela Proposta, e do outro que a expectativa de a Europa poder tomar um papel dianteiro no percurso tecnológico mundial poderá ter caído por terra face a uma regulamentação (eventualmente) demasiado intrincada. Urge, pois, identificar quais as fragilidades desta Proposta para perceber o que nos espera e trabalhar para a sua futura correcção.

## PALAVRAS-CHAVE

inteligência artificial, União Europeia, tecnologia, direitos fundamentais.

---

<sup>3</sup> Professora na Faculdade de Direito da Universidade de Coimbra, [vera@fd.uc.pt](mailto:vera@fd.uc.pt)



---

# Draft Regulation on Artificial Intelligence: The devil is in the details

*Vera Lúcia Raposo*

## **ABSTRACT**

The European Commission's recent proposal for a legal framework on artificial intelligence in the European Union – the so-called Artificial Intelligence Regulation – was received with enthusiasm, but also with apprehension and some disappointment. Enthusiasm because a legal stand from the European Union in this regard has long been expected as a way of boosting the European digital project. Apprehension because the effects of artificial intelligence on the fundamental rights of European citizens are feared. Disillusionment, which is double, because on the one side it is argued that fundamental rights were not safeguarded by the Proposal, and on the other side that the expectation of watching Europe taking a leading role in the world's technological path may have fallen apart in face of a regulation (eventually) too intricate. It is therefore urgent to identify the weaknesses of this Proposal in order to understand what is coming ahead and work for its future correction.

## **KEYWORDS:**

artificial intelligence, European Union, technology, fundamental rights.

## 1. Apresentação geral da Proposta sobre Inteligência Artificial

Quando, em Abril de 2021, a Comissão Europeia divulgou a sua proposta (doravante, a 'Proposta') para um futuro regulamento da União Europeia (UE) sobre Inteligência Artificial (IA)<sup>4</sup> experts e stakeholders de todo o mundo sustiveram a respiração. A curiosidade era grande (apesar de o Livro Branco,<sup>5</sup> que precedeu a dita proposta, ter já lançado algumas luzes sobre o que aí viria) e a ansiedade de quem criou um negócio com base na tecnologia de IA não era menor. O caso não é para menos. O teor da futura regulamentação europeia sobre a IA poderá ditar o sucesso (ou o fracasso) de muitos projectos (empresariais e não só) na Europa e para além dela (por força dos efeitos extraterritoriais da Proposta).

O objectivo primacial da Proposta é facilitar e desenvolver o uso de IA na UE para criar um verdadeiro Mercado Único Digital,<sup>6</sup> uma aspiração desde há muito apregoada. Porém, este objectivo pode ver a sua realização limitada por outra aspiração da Proposta: a protecção dos direitos fundamentais, dos valores europeus e dos princípios éticos potencialmente ameaçados pela IA.<sup>7</sup> Resta saber se a esperada compatibilização de finalidades é efectivamente cumprida por esta Proposta.

O presente estudo irá centra-se nos segmentos da Proposta que – justificada ou injustificadamente – mais celeuma têm causado. É sabido que nunca se pode agradar a todos e casos há em que a mesma norma foi atacada de quadrantes opostos, por proteger de menos ou por proteger demais. Afinal, há diferentes tipos de interesses a digladiarem-se neste campo e nem sempre é fácil, ou até possível, satisfazer a todos.

## 2. Definição de IA

O que se entendia por IA nos anos 60 dificilmente conseguiria abarcar a realidade hodierna.<sup>8</sup> Muitas definições têm sido apresentadas sobre o conceito de IA. Por exemplo, a Autoridade Norueguesa de Protecção de Dados, num relatório de 2018, apresentou a seguinte definição: 'Artificial intelligence (AI) is the concept used to describe computer systems that are able to learn from their own experiences and solve complex problems in different situations – abilities we previously thought were unique to

---

<sup>4</sup> PARLAMENTO EUROPEU E CONSELHO, **Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento inteligência artificial) e altera determinados atos legislativos da união**, 21/04/2021, COM/2021/206 final, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>.

Neste estudo vou-me escusar de apresentar de novo a proposta, dada a ampla proliferação de textos nesse sentido, não apenas em inglês (RAPOSO, Vera Lúcia. **May I Have Some Artificial Intelligence with My Human Rights? About the Recent European Commission's Proposal on a Regulation for Artificial Intelligence**. KSLR EU Law Blog, May 24 2021. Retrieved 12 June 2021, <https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1569>), mas também em português (CALDEIRA, Cristina Maria de Gouveia. **Regulamento Inteligência Artificial**. Privacy and Data Protection Magazine, n. 2, pp. 164-167, 2021).

<sup>5</sup> EUROPEAN COMMISSION, **White paper on Artificial Intelligence - A European approach to excellence and trust**, Brussels, 19.2.2020 COM(2020) 65 final, [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf)

<sup>6</sup> EU4DIGITAL, **EU Digital Single Market**, <https://eufordigital.eu/discover-eu/eu-digital-single-market/>.

<sup>7</sup> Neste sentido, RAPOSO, op. cit.

<sup>8</sup> SWEDSOFT, **Comments Regarding the European Commission's proposal for an Artificial Intelligence Act**, 24 June 2021, <https://www.regeringen.se/49eb04/contentassets/59dff9749d5e4cfa8d51146dd026ff62/swedsoft.pdf>, p. 2

mankind. And it is data, in many cases personal data, that fuels these systems, enabling them to learn and become intelligent'.<sup>9</sup> A Amazon, uma multinacional tecnológica que reconhecidamente se desenvolveu com base na IA, fornece a seguinte definição no seu website: 'Inteligência artificial é um campo da ciência da computação dedicado a resolver problemas cognitivos geralmente associados à inteligência humana, como aprendizado, solução de problemas e reconhecimento de padrões. Embora a inteligência artificial, geralmente abreviada como "IA", nos remeta a robôs e cenas futuristas, ela vai muito além dos autômatos da ficção científica, abrangendo o mundo não fictício da ciência da computação avançada da modernidade (...) O machine learning (ML) e o aprendizado profundo (DL) são campos da ciência da computação derivados da disciplina da inteligência artificial'.<sup>10</sup> As possíveis definições são, pois, ilimitadas.

Até esta Proposta, a definição em vigor na UE era aquela formulada pela Comissão Europeia em 2018: 'Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals'.<sup>11</sup>

Em contrapartida, a Proposta da Comissão Europeia adota um modelo a dois tempos para fornecer uma definição de IA. Primeiro, no Artigo 3, apresenta um conceito (curiosamente, não de IA, mas de 'sistemas de IA'), relativamente vago e genérico: "Sistema de inteligência artificial" (sistema IA), um programa de computador desenvolvido com uma ou mais das técnicas e abordagens enumeradas no Anexo I, capaz de gerar resultados, tendo em vista um determinado conjunto de objetivos definidos pelo ser humano. conteúdos, previsões, recomendações ou decisões que influenciam os ambientes com os quais interage'. Seguidamente, esta definição-umbrela é densificada mediante os exemplos elencados no Anexo I, para os quais remete o Artigo 4 da Proposta, e que lista as técnicas e abordagens no domínio da IA abarcados pelo seu regime: 'Abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda; b) Abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais; c) Abordagens estatísticas, estimação de Bayes<sup>12</sup>, métodos de pesquisa e otimização'.

Um primeiro reparo é a ausência de distinções relevantes. Por exemplo, a Swedsoft alega que a definição não faz qualquer distinção entre, por um lado, algoritmos e dados e, por outro lado, os modelos construídos com combinações de

---

<sup>9</sup> DATATYLSINET, **Artificial intelligence and privacy report**. Datatylsinet, 2018, p. 5, <https://www.datatylsinet.no/globalassets/global/english/ai-and-privacy.pdf>.

<sup>10</sup> AMAZON, **O que é inteligência artificial?**, nd, <https://aws.amazon.com/pt/machine-learning/what-is-ai/>

<sup>11</sup> EUROPEAN COMMISSION, **Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe**, Brussels, 25.4.2018 COM(2018) 237 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

<sup>12</sup> Uma das críticas apontadas é que a estimação de Bayes é um teorema matemático e não uma 'técnica ou abordagem' de inteligência artificial (GAUMOND, Eve, **Artificial Intelligence Act: What is the European approach for AI?**, June 4, 2021, Lawfare, <https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai/>).

algoritmos e dados; nem entre os diferentes tipos de algoritmos e os diferentes tipos de dados.<sup>13</sup> Tudo entra na referida definição geral de IA.

A Proposta peca também pelo seu carácter demasiado lato. É mais ampla do que a maioria das definições de IA, o que fará com que software não comumente considerado como usando IA seja coberto pelo futuro Regulamento. A definição de IA utilizada é apresentada como sendo suficientemente ampla para abranger futuros desenvolvimentos desta tecnologia e assim não ficar ultrapassada. Porém, outro possível cenário é que uma definição tão abrangente se torne simplesmente inaplicável a qualquer sistema específico.<sup>14</sup> De qualquer modo, por muito ampla que seja a definição, mais cedo ou mais tarde acabará por ficar ultrapassada, dado que a tecnologia corre sempre mais rápido do que qualquer definição legal.

### 3. Falhas na categorização dos níveis de risco

O reconhecimento dos riscos inerentes à IA é um dado adquirido, chegando inclusivamente de quadrantes insuspeitos.<sup>15</sup> Não espanta, pois, que a Proposta funde as suas soluções nas categorizações dos possíveis riscos de cada sistema (tal como, de resto, já sucede noutros textos similares,<sup>16</sup> desde logo no Regulamento Geral de Protecção de Dados, doravante RGPD).<sup>17</sup>

A quantidade e qualidade (gravidade) das exigências a que cada sistema de IA será sujeito depende, no quadro da Proposta, dos respectivos níveis de risco.<sup>18</sup> Assim, distinguem-se:

- (a) Sistemas de IA de risco inaceitável, os quais são proibidos;
- (b) Sistemas de IA de alto risco, permitidos, embora dentro de apertadas exigências;
- (c) Sistemas de IA de baixo risco. Nestes tem-se distinguido<sup>19</sup> – a própria Comissão Europeia procedeu a esta distinção<sup>20</sup> – entre sistemas de risco limitado e de risco mínimo, embora esta subdistinção, e respectivas consequências, não resulte clara da Proposta.

Porém, a categorização dos níveis de risco suscita algumas questões:

---

<sup>13</sup> SWEDSOFT, cit, p. 3.

<sup>14</sup> SWEDSOFT, cit, p. 2.

<sup>15</sup> Renomados perfis da ciência, como Stephen Hawking (GRIFFIN, Andrew, **Stephen Hawking: Artificial intelligence could wipe out humanity when it gets too clever as humans will be like ants**, Independent, 8 October 2015, <https://www.independent.co.uk/life-style/gadgets-and-tech/news/stephen-hawking-artificial-intelligence-could-wipe-out-humanity-when-it-gets-too-clever-humans-could-become-ants-being-stepped-06686496.html>) e Elon Musk (PIPER, Kelsey, Why Elon Musk fears artificial intelligence, Vox, Nov 2, 2018, <https://www.vox.com/future-perfect/2018/11/2/18053418/elon-musk-artificial-intelligence-google-deepmind-openai>) já se pronunciaram a este respeito, sublinhando os riscos que daqui podem advir.

<sup>16</sup> ARTICLE 29 DATA PROTECTION WORKING PARTY, **Statement on the role of a risk-based approach in data protection legal frameworks**, adopted on 30 May 2014, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf).

<sup>17</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados).

<sup>18</sup> Sobre a regulação fundada no risco (risk-based approach), em particular no domínio da protecção de dados, veja-se GELLERT, Raphaël, **The risk-based approach to data protection**. Oxford University Press, 2020, que no capítulo I (pp. 26-53) fornece uma apresentação desta abordagem. O capítulo VII (pp. 212-238) refere-se às suas várias particularidades e ressalvas, com considerações que podem ser transpostas para a presente problemática.

<sup>19</sup> GAUMOND, cit.; VEALE, Michael, BORGESIU, Frederik, **Demystifying the draft EU Artificial Intelligence Act - Analysing the good, the bad, and the unclear elements of the proposed approach**, Computer Law Review International, vol. 22, no. 4, 2021, pp. 97-112. <https://doi.org/10.9785/crl-2021-220402>, p. 3

<sup>20</sup> EUROPEAN COMMISSION, **New rules for Artificial Intelligence – Questions and answers**, 21 April 2021, [https://ec.europa.eu/commission/presscorner/detail/en/QANDA\\_21\\_1683](https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683)

Primeiro, alega-se que a definição dos níveis de risco centra-se demasiado no respectivo software, descurando o seu hardware. Esta foi uma preocupação suscitada pela ANEC (European Consumer Voice in Standardisation), que fornece o seguinte exemplo ilustrativo: os softwares de reconhecimento facial fundados na IA funcionam conectados a uma câmara, a qual, sendo uma câmara simples, de baixa resolução, envolve menor risco do que tratando-se de câmaras de alto desempenho ou com visão nocturna.<sup>21</sup> Eis um exemplo de como o hardware pode condicionar profundamente o desempenho do software. Porém, não é claro que a Proposta tenha tido em consideração estes condicionamentos na delimitação dos níveis de risco.

Um outro possível problema resulta do conceito de 'finalidade prevista' (para os sistemas de IA), repetidamente invocada ao longo da Proposta. Ora, alega-se - de novo a ANEC -<sup>22</sup> que do ponto de vista dos consumidores o que releva não é a finalidade prevista, mas a previsível (rectius, as previsíveis), a qual, por sua vez, deve ser avaliada de acordo com as características técnicas e funcionais do sistema de IA, os comportamentos factuais e humanos, e a utilização conjunta com outros produtos. Por conseguinte, o que deve nortear as avaliações de risco são os usos que sejam razoavelmente previsíveis, ainda que não se trate de usos previstos.<sup>23</sup>

#### 4. As proibições flexíveis

A proposta apresenta-se como proibindo sistemas de IA considerados especialmente ameaçadores para os direitos das pessoas, mas este anúncio de intenções nem sempre tem as necessárias consequências práticas.

Por exemplo, o Artigo 5 encerra uma proibição – supostamente absoluta – relativamente a vários sistemas de IA considerados de risco inaceitável. Porém, uma análise mais cuidada das normas deixa antever que a proibição afinal admite várias brechas. Vejamos alguns exemplos paradigmáticos desta técnica de 'proibição/ afinal não':

- i) Os sistemas de IA considerados manipuladores - tal como definido no Artigos 5/1/a e Artigos 5/1/b, de acordo com o Considerando 15 da Proposta – são, supostamente, totalmente proibidos. Porém, a forma como estão definidos deixa várias situações de fora. Desde logo, porque as normas em apreço exigem a intenção manipulativa da pessoa ou entidade que desenvolve, comercializa ou usa estes sistemas de IA.<sup>24</sup> Contudo, o que sucede caso essa intenção não seja declarada? Convenhamos que poucos destes agentes irão expressamente afirmar que usam a IA para efeitos de manipular comportamentos e emoções. Não é inusual encontrar no mercado produtos vendidos para determinado fim, mas que todos sabem, incluindo produtores e vendedores, ser usados para outros fins.<sup>25</sup> Por outro lado, fazer prova de intenções não declaradas de forma expressa (mas apenas deduzidas de comportamentos) é extremamente complicado, pelo que resta ver como irão as entidades competentes actuar no âmbito

---

<sup>21</sup> EUROPEAN CONSUMER VOICE IN STANDARDISATION (ANEC), **ANEC commentson the European Commission proposal for an Artificial Intelligence Act.** Position Paper. July 2021. <https://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2021-G-071.pdf>

<sup>22</sup> EUROPEAN CONSUMER VOICE IN STANDARDISATION (ANEC), cit.

<sup>23</sup> Para além do uso a que um produto se destina, e para o qual foi comercializado, pode o mesmo ter outros usos. Por exemplo, os monitores para bebés podem ser usados como câmaras de vigilância (LAUGHLIN, Andrew, **Which? Warns parents not to use a security camera as a baby monitor**, 24 Jul 2020, <https://www.which.co.uk/news/2020/07/which-warns-parents-not-to-use-a-security-camera-as-a-baby-monitor/>).

<sup>24</sup> A alínea a) refere 'para'; a alínea b) usa a expressão 'a fim de'. Veja-se ainda o enfoque do Considerando 16 na 'intenção'.

<sup>25</sup> Recordemos a dicotomia usos possíveis versus usos previstos. Para além dos já referidos casos de monitores para monitorizar bebés e/ou vigiar pessoas, suponha-se ainda o caso de um brinquedo que 'fala' com as crianças usando IA, aparentemente educativo, mas que na realidade visa doutrina-las para determinada religião.

deste Regulamento e como irá a jurisprudência comunitária aplicar este requisito. Por outro lado, ainda, não é claro se o dano exigido por ambas as alíneas ('cause ou seja susceptível de causar danos físicos ou psicológicos a essa ou a outra pessoa') tem que ser provocado por um único evento capaz de produzir um efeito manipulatório, ou se pode ser causado por uma sequência de eventos, nenhum deles por si suficiente para causar tal efeito, mas já possível quando actuam em conjunto, como será de resto habitual em muitos casos de sistemas de IA manipuladores.<sup>26</sup>

- ii) Outra das proibições flexíveis prende-se com a tecnologia de reconhecimento facial para fins de investigação criminal em espaços públicos em tempo real. No Artigo 5/1/d a Proposta parece conter uma proibição total, mas logo de seguida permite várias excepções a esta proibição. Teme-se que num clima de insegurança generalizada como é o actual, e arvorando-se em finalidades preventivas, câmaras de reconhecimento facial acabem por ser instaladas em vários espaços públicos.<sup>27</sup> A tecnologia de reconhecimento facial aporta muitos benefícios em sede de law enforcement,<sup>28</sup> sobretudo considerando que os criminosos não olham a meios para realizar os seus intentos, cujos efeitos podem ser mais nefastos do que os resultantes do uso desta tecnologia. Porém, em jurisdições com tiques de estado autoritário – e também as temos na Europa<sup>29</sup> – este pode ser um perigoso retrocesso para alguns direitos fundamentais,<sup>30</sup> tanto mais que embora seja em regra exigida prévia autorização judicial para o uso desta tecnologia, a mesma pode ser adiada em caso de urgência (Artigo 5/3 da Proposta).
- iii) Na sua opinião conjunta,<sup>31</sup> quer o European Data Protection Board quer o European Data Protection Supervisor advogaram que não deveria existir qualquer excepção à proibição da identificação biométrica remota de indivíduos em espaços públicos (rostos, marcha, pegada digital, reconhecimento de voz, etc.).<sup>32</sup> Contudo, uma tal solução impediria o uso de um poderoso e útil mecanismo de investigação policial, que não podemos simplesmente desaproveitar. A melhor solução reside em manter algumas proibições, limitações, regulamentação e monitorização, mas não impor uma proibição absoluta.
- iv) Outra solução de proibição excessivamente flexível prende-se com a avaliação de conformidade dos sistemas de IA. Os sistemas de IA de alto risco estão sujeitos à marcação de conformidade CE<sup>33</sup> para poderem ser comercializados (Considerando 67 e Artigos 16/i, 19/1, 26/1/c e 27/1 da Proposta). Ao invés do que sucede no âmbito de outros modelos de conformidade - veja-se o caso dos medicamentos<sup>34</sup> - a avaliação de

---

<sup>26</sup> Cfr. VEALE, BORGESIUŠ, cit., p. 4

<sup>27</sup> MENECEUR, Yannick, **European Commission's Alregulation proposal: between too much and too little?**, April 23, 2021, <https://www.linkedin.com/pulse/european-commissions-ai-regulation-proposal-between-too-meneceur/>.

<sup>28</sup> Veja-se MCCLELLAN, Elizabeth, **Note, Facial Recognition Technology: Balancing the Benefits and Concerns**, Bus. & Tech. L. vol. 15, 2020, pp. 363-380, at 371-374.

<sup>29</sup> Por exemplo, na Hungria as câmaras de reconhecimento facial são usadas para controlo do tráfego rodoviário. Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, **Facial recognition technology: fundamental rights considerations in the context of law enforcement**. Publication Office of the European Union, 2019, p. 3.

<sup>30</sup> EDRI, **From 'trustworthy AI' to curtailing harmful uses: EDRI's impact on the proposed EU AI Act**, June 1 2021, <https://edri.org/our-work/from-trustworthy-ai-to-curtailing-harmful-uses-edris-impact-on-the-proposed-eu-ai-act/>.

<sup>31</sup> EUROPEAN DATA PROTECTION BOARD AND EUROPEAN DATA PROTECTION SUPERVISOR, **Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)**, 18 June 2021, [https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en), pp. 11-12.

<sup>32</sup> Nesta sua opinião, ambas entidades recomendam igualmente a proibição de sistemas biométricos usados para classificar indivíduos em grupos com base na respectiva etnia, sexo, orientação política ou sexual ou outros motivos pelos quais a discriminação está proibida ao abrigo do artigo 21.º da Carta dos Direitos Fundamentais da União Europeia (EUROPEAN DATA PROTECTION BOARD AND EUROPEAN DATA PROTECTION SUPERVISOR, cit, p. 12). Esta é uma crítica pertinente, dado que não se vislumbra nenhum cenário onde tal classificação seja relevante.

<sup>33</sup> Sobre a marcação CE veja-se a Decisão n. 768/2008/CE (PARLAMENTO EUROPEU E CONSELHO, **Decisão n. 768/2008/CE do Parlamento Europeu e do Conselho, de 9 Julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE**, <https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32008D0768>).

<sup>34</sup> Quem controla a qualidade (eficácia e segurança) dos medicamentos não são as próprias companhias farmacêuticas, mas as autoridades nacionais do medicamento ou a Agência Europeia do Medicamento, como resulta da Directiva 2001/83/CE do Parlamento Europeu e do Conselho, de 6 de Novembro de 2001, que estabelece um código comunitário relativo aos medicamentos para uso humano, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001L0083>.



conformidade dos sistemas de IA com os requisitos legais pode, em alguns casos, ser levada a cabo pelos próprios fabricantes. Esta solução tem aspectos positivos, dado que o fabricante é quem melhor conhece o seu produto e, por conseguinte, quem melhor pode atestar a sua conformidade. Contudo, tem um inegável problema: como confiar num sistema em que a entidade sob controlo, ainda para mais controlo de uma actividade/produto de alto risco, se controla a si própria?

- v) Nem mesmo a intervenção dos chamados organismos notificados para levar a cabo a avaliação de conformidade nos sistemas de IA de alto risco (Artigos 30 e seguintes da Proposta) confere tranquilidade quanto ao tipo de controlo feito. Em teoria, estes organismos serão entidades independentes, operando de forma autónoma e transparente (na prática pouco se sabe da forma como desempenham as suas funções).<sup>35</sup> Contudo, teme-se que os organismos notificados se resumam a companhias privadas, criando aquilo a que já se chamou 'privatised compliance industry'.<sup>36</sup> Há o perigo de estas entidades se preocuparem apenas em fazer que os sistemas de IA sejam aprovados dentro do respeito formal das exigências da Proposta, descurando a defesa dos direitos dos envolvidos.<sup>37</sup>

## 5. As exigências impossíveis

Se por um lado a Proposta é demasiado 'flexível' em matérias onde deveria ter sido mais cautelosa, por outro lado, há domínios onde peca pelo excesso de rigidez, de complexidade regulamentadora e pela exigência de standards difíceis de atingir na prática. Algumas matérias focadas pela Proposta não só são altamente regulamentadas, como ademais sujeitas a padrões de exigência excessivamente rígidos e, eventualmente, impossíveis de cumprir.

Por exemplo, o Artigo 10/3 estipula que 'os conjuntos de dados de treino, validação e teste devem ser pertinentes, representativos, isentos de erros e completo' (a mesma ideia resulta do Considerando 44 da Proposta). Ora, os especialistas salientam que um conjunto de dados completamente livre de erros é utópico.<sup>38</sup>

À dificuldade no seu cumprimento acresce a ambiguidade de tal exigência.<sup>39</sup> Será que o erro em causa se refere ao conjunto dos dados, à sua classificação, à forma como o comportamento pretendido é representado, a todos estes aspectos, ou ainda a outros? Por outro lado, quem avalia a qualidade dos dados e com que critérios?

As obrigações de transparência – constantemente invocadas na Propostas<sup>40</sup> - são outro desses exemplos. Dado que falamos de uma tecnologia

---

<sup>35</sup> GALLAND, Jean-Pierre, **The difficulties of regulating markets and risks in Europe through notified bodies**, European Journal of Risk Regulation, vol. 4, n. 3, 2013, pp. 365-373, p. 369, Doi: <https://doi.org/10.1017/S1867299X00002634>; VEALE, Michael, BORGESIU, Frederik, cit., p. 15.

<sup>36</sup> Preocupação apontada por Daniel Leufer, analista de políticas digitais no espaço europeu e membro do grupo de direitos humanos Access Now, citado em SKELTON, Sebastian Klovig, **Europe's proposed artificial intelligence regulation falls short on protecting rights**, computerweekly.com, 22-28 June 2021, <https://www.computerweekly.com/feature/Europes-proposed-AI-regulation-falls-short-on-protecting-rights>, p. 7.

<sup>37</sup> De novo Daniel Leufer, citado em SKELTON, cit., p. 7.

<sup>38</sup> SIEMENS, **EU's AI Regulation proposal (21/04/2021) Position & recommendations**, July 2021, [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662941\\_en?fbclid=IwAR1W6QQXasZgrCkZM5Z9W22JVFg0RDrh-gc4dFIXvg8z-z-fAhAQi66y39Y](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662941_en?fbclid=IwAR1W6QQXasZgrCkZM5Z9W22JVFg0RDrh-gc4dFIXvg8z-z-fAhAQi66y39Y), p. 3.

<sup>39</sup> SIEMENS, cit., p. 6.

<sup>40</sup> Considerandos 14, 38, 39, 43, 47, 69 e 70, Artigos 1/d e 13, e Título IV da Proposta.

opaca (a famosa black box),<sup>41</sup> até onde podem ir tais obrigações e quais as consequências práticas do cumprimento destas obrigações?

## 6. Matérias omissas na Proposta

A Proposta pretende ser uma regulamentação abrangente sobre IA, mas ficou aquém deste desejo. Certamente que seria impossível pretender regular todo e qualquer detalhe relacionada com a IA – aliás, a hiper-regulamentação é, porventura, um dos maiores problemas da Proposta – mas há questões que não podem de ficar de fora de uma regulamentação que se pretende completa e não-fragmentada.

Entre os mais 'gritantes' pontos omissos veja-se a questão da responsabilidade por produtos defeituosos que operem com IA. A questão da responsabilidade do produtor vem actualmente regulada na Directiva n.º 85/374/CEE,<sup>42</sup> sobre responsabilidade decorrente de produtos defeituosos, que na verdade está em vias de ser revista com o propósito de a adequar aos novos desafios do mundo digital,<sup>43</sup> e onde se espera que apareçam soluções adequadas ao uso da IA em vários produtos.<sup>44</sup> Em 2020, já o Parlamento Europeu tinha apresentado a sua Resolução sobre o regime de responsabilidade civil aplicável à IA.<sup>45</sup> Seria de esperar que a Proposta abarcasse esta importante questão, mas curiosamente deixou-a de fora.

A isto acresce que a Proposta não estabelece um direito legal de actuar judicialmente contra os fornecedores ou utilizadores de sistemas de IA pelo não cumprimento das suas normas (ainda que a desconformidade com as referidas normas possa ser invocada num processo de responsabilidade civil). Esta tem sido uma crítica reiteradamente apontada, quer por autoridades europeias (como o European Data Protection Board e o European Data Protection Supervisor)<sup>46</sup> quer por grupos civis de defesa de direitos.<sup>47</sup>

---

<sup>41</sup> Cassauwers, Tom, **Opening the 'black box' of artificial intelligence**, Horizon . The EU Research and Innovation Magazine, 01 December 2020  
<https://ec.europa.eu/research-and-innovation/en/horizon-magazine/opening-black-box-artificial-intelligence>

<sup>42</sup> Directiva do Conselho de 25 de Julho de 1985 relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-membros em matéria de responsabilidade decorrente dos produtos defeituosos (Directiva 85/374/CEE).

<sup>43</sup> Sobre a revisão desta Directiva vide EUROPEAN COMMISSION, **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence**, 21/04/2021, COM/2021/205 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:205:FIN>.

<sup>44</sup> Entre as soluções 'taylor-made' para produtos que operem à base de IA que já foram advogadas encontra-se a inversão do ónus da prova em caso de litígio por produto defeituoso, dado o desequilíbrio de forças (e de conhecimento) entre os fornecedores, vendedores e utilizadores desta tecnologia e aqueles que são afectados por ela. Cfr. SKELTON, cit., p. 11.

<sup>45</sup> PARLAMENTO EUROPEU, **Resolução do Parlamento Europeu, de 20 de Outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial (2020/2014(INL))**, [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_PT.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PT.pdf)

<sup>46</sup> EUROPEAN DATA PROTECTION BOARD AND EUROPEAN DATA PROTECTION SUPERVISOR, cit., par. 18.

<sup>47</sup> SKELTON, cit., p. 11.



## 7. Conflitos entre normas e jurisdições

Com várias normas a regular o mesmo assunto e vários possíveis tribunais a poder dirimir eventuais litígios, é natural que ocorram conflitos de normas e de jurisdições.

Relativamente ao patchwork de normas que se antevê no futuro, sublinhe-se que esta Proposta surge no âmbito de um projecto bem mais vasto, que pretende trazer a UE para o mundo digital. Para este efeito, vários projectos estão neste momento na calha: o Regulamento dos serviços digitais,<sup>48</sup> o Regulamento dos mercados digitais,<sup>49</sup> o Regulamento relativo às máquinas e seus componentes e acessórios<sup>50</sup> e o Regulamento da governação de dados.<sup>51</sup> A tudo isto acresce outro vasto rol de diplomas já existentes e igualmente pertinentes para o domínio da IA: o RGPD, a Directiva sobre protecção de dados em matéria criminal,<sup>52</sup> a Directiva relativa à privacidade e às comunicações electrónicas,<sup>53</sup> o Regulamento sobre dispositivos médicos<sup>54</sup>, o Regulamento sobre dispositivos de diagnóstico in vitro,<sup>55</sup> a anunciada revisão da Directiva sobre produtos defeituosos, apenas para referir alguns exemplos.

Será quase impossível que não haja sobreposições entre todos estes documentos legais. Ainda que as respectivas normas não entrem em conflito, permanece o desafio de as ter a todas em consideração no momento de actuar ou de decidir. Tomemos um exemplo concreto: dado que os sistemas de IA funcionam com dados, boa parte deles dados pessoais, será necessário articular o RGPD com o Regulamento de IA, o que não será tarefa simples, dado que ambos incluem normas muito detalhadas na sua regulamentação.

Acrescente-se ainda que várias das proibições da Proposta pouco acrescentam ao que já resulta do direito europeu. Por exemplo, algumas das

---

<sup>48</sup> PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais (Regulamento Serviços Digitais) e que altera a Directiva 2000/31/CE**, Bruxelas, 15.12.2020, COM(2020) 825 final, 2020/0361(COD) (<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0825&from=en>).

<sup>49</sup> PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à disputabilidade e equidade dos mercados no sector digital (Regulamento Mercados Digitais)**, Bruxelas, 15.12.2020, COM(2020) 842 final, 2020/0374(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0842&from=en>.

<sup>50</sup> PARLAMENTO EUROPEU E CONSELHO, **Regulamento do Parlamento Europeu e do Conselho relativo às máquinas e seus componentes e acessórios**, Bruxelas, 21.4.2021, COM(2021) 202 final, 2021/0105(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0202&from=EN>.

<sup>51</sup> PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados)**, Bruxelas, 25.11.2020, COM(2020) 767 final, 2020/0340(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0767&from=EN>.

<sup>52</sup> Directiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

<sup>53</sup> Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), processo de revisão.

<sup>54</sup> Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho de 5 de Abril de 2017 relativo aos dispositivos médicos, que altera a Directiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Directivas 90/385/CEE e 93/42/CEE do Conselho.

<sup>55</sup> Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho de 5 de Abril de 2017 relativo aos dispositivos médicos para diagnóstico in vitro e que revoga a Directiva 98/79/CE e a Decisão 2010/227/UE da Comissão.

proibições de práticas manipulatórias por meio de IA decorriam já da Directiva relativa às práticas comerciais desleais,<sup>56</sup> a qual proíbe, por deslealdade, toda a prática comercial que 'distorcer ou for susceptível de distorcer de maneira substancial o comportamento económico, em relação a um produto, do consumidor médio a que se destina ou que afecta, ou do membro médio de um grupo quando a prática comercial for destinada a um determinado grupo de consumidores' (Artigo 5/2/b).

Quanto ao conflito entre jurisdições, antevê-se que alguns dos 'choques' que já hoje ocorrem no âmbito do RGPD entre vários tribunais venham a repetir-se no contexto da futura regulamentação sobre IA.<sup>57</sup> Em causa estão matérias administrativas, criminais e cíveis e, por conseguinte, os respectivos tribunais.

Este conflito será igualmente patente no âmbito das entidades competentes para proceder à harmonização e controlo dos sistemas de IA. A Proposta exige a criação de órgãos específicos a nível nacional (autoridades notificadoras e organismos notificados), bem como a nível europeu, nomeadamente o Comité Europeu de Inteligência Artificial. Este último é uma autoridade de supervisão supranacional, semelhante ao Comité Europeu para a Protecção de Dados, criado sob a égide do RGPD, e também ao Conselho Europeu de Serviços Digitais, referido na proposta de Regulamento dos serviços digitais. Algumas entidades nacionais de protecção de dados já fizeram saber que consideram ser elas as mais indicadas para funcionar como entidades supervisoras dos sistemas de IA.<sup>58</sup> Alegam que fazer uso de autoridades já sedimentadas e com experiência neste tipo de controlo (dado o já referido uso de dados pessoais por parte dos sistemas de IA é comum que tais entidades sejam chamadas a pronunciar-se sobre os mesmos) traria maior eficácia ao modelo regulatório. Por outro lado, argumentam que assim se reduziria a insegurança jurídica e a complexidade administrativa, dado que seria possível obter maior coerência entre as soluções dadas à luz do Regulamento de IA e as dadas à luz do RGPD (e, já agora, da Directiva 2016/680, cujo controlo está igualmente na competência das autoridades nacionais de protecção de dados).

---

<sup>56</sup> Directiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de Maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Directiva 84/450/CEE do Conselho, as Directivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.º 2006/2004.

<sup>57</sup> MENECEUR, cit.

<sup>58</sup> COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), **Artificial intelligence: the opinion of the CNIL and its counterparts on the future European regulation**, 8 July 2021, <https://www.cnil.fr/en/artificial-intelligence-opinion-cnil-and-its-counterparts-future-european-regulation>.

Outra vantagem é que se evitaria a multiplicação de autoridades de supervisão. Não se contestando as vantagens apontadas à centralização de poderes e funções nas entidades nacionais de protecção de dados, parece-me, porém, que o raciocínio que subjaz à protecção de dados não coincide inteiramente com o raciocínio necessário para monitorizar os sistemas de IA. Ou seja, a IA suscita muitas outras questões para além daquelas típicas da protecção de dados. Porém, o reconhecimento desta especificidade trará inevitavelmente sobreposições de competências.

## 8. A competitividade tecnológica

Apesar de alguns críticos apontarem o teor excessivamente 'business' da Proposta, ela parece-me na verdade mais propensa à protecção de direitos do que ao alavancamento tecnológico. Ora, esta 'propensão' é, obviamente, louvável. Porém, cabe perguntar que espaço de manobra é deixado às start-up's europeias? Aparte os ambientes de testagem (as 'regulatory sandboxes', referidas nos Artigos 53 e 54 da Proposta) e as medidas de incentivo aos pequenos e médios fornecedores de IA (Artigo 55 da Proposta), não há muito encorajamento à inovação tecnológica.

Se, como tudo indica, o conteúdo da Proposta se tornar no Regulamento de IA da UE, o que se pode esperar é que a investigação, fabrico e comercialização de IA no espaço europeu sofra um duro golpe, especialmente nos primeiros tempos, enquanto a máquina não estiver oleada. Um problema que desde logo se antevê é o da *compliance* com tantas e tão pormenorizadas regras (não apenas as do futuro Regulamento sobre IA, mas todas as outras normas relevantes). Conseguirá um investigador, um fabricante, um empreendedor, fazer face a tantas exigências simultâneas e eventualmente conflitantes?

Atrevo-me a fazer um paralelismo com o que sucede em relação ao RGPD. Ninguém contesta que o nível de exigência em termos de requisitos e de limitações ao que pode ser feito está praticamente no limite máximo. O detalhe na regulamentação (hiper-regulamentação) não tem equivalente no resto do mundo. Dito isto, em termos de resultado práticos, será que estão os dados pessoais dos europeus mais protegidos do que noutras jurisdições?

Temo que a Regulamentação de IA se torna também ela uma hiper-regulamentação, com regras massivas sobre praticamente tudo, limitações que impedem o desenvolvimento de novas tecnologias, burocracias excessivas, proibições absurdas,<sup>59</sup> sanções pesadíssimas, sem que no final daqui decorra necessariamente maior protecção para os direitos das pessoas.

---

<sup>59</sup> IRISH DATA PROTECTION COMMISSION, **Taking photos at school events – Where common sense comes into play**, 12th April 2019, <https://www.dataprotection.ie/en/dpc-guidance/blogs/taking-photos-school-events-where-common-sense-comes-play>

Entretanto, e enquanto a EU se debate com exigências minuciosas e intrincadas, o resto do mundo continuará o seu rumo face ao digital. A UE poderá não conseguir apanhar o comboio da transformação tecnológica,<sup>60</sup> pelo menos não num futuro próximo.<sup>61</sup>

## 9. Considerações finais

O esforço da Comissão Europeia é meritório, como meritória é a Proposta que apresentou. Porém, não há trabalhos perfeitos, e o nível de imperfeição aumenta na exacta medida em que aumenta a ambição de um projecto. A Proposta é um projecto ambicioso, tanto pelo seu âmbito de aplicação como pelo seu nível de detalhe, ao que acresce ainda a complexidade de um domínio muito novo. Logo, seria quase impossível não haver falhas nas suas minúcias, como precisamente este breve estudo tentou apontar. The devil is in the details.

---

<sup>60</sup> A mesma preocupação em RAPOSO, cit.

<sup>61</sup> Veja-se o enorme poder em AI do colosso chinês. Cfr. LI, Daitian, TONG, Tony W., XIAO, Yangao, **Is China emerging as the global leader in AI?**, Harvard Business Review, February 18, 2021, <https://hbr.org/2021/02/is-china-emerging-as-the-global-leader-in-ai>

## 10. Bibliografia

- AMAZON, **O que é inteligência artificial?**, nd, <https://aws.amazon.com/pt/machine-learning/what-is-ai/>
- ARTICLE 29 DATA PROTECTION WORKING PARTY, **Statement on the role of a risk-based approach in data protection legal frameworks**, adopted on 30 May 2014, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf)
- CALDEIRA, Cristina Maria de Gouveia. **Regulamento Inteligência Artificial**. Privacy and Data Protection Magazine, n. 2, pp. 164-167, 2021
- CASSAUWERS, Tom, **Opening the 'black box' of artificial intelligence**, Horizon . The EU Research and Innovation Magazine, 01 December 2020 <https://ec.europa.eu/research-and-innovation/en/horizon-magazine/opening-black-box-artificial-intelligence>
- COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), **Artificial intelligence: the opinion of the CNIL and its counterparts on the future European regulation**, 8 July 2021, <https://www.cnil.fr/en/artificial-intelligence-opinion-cnil-and-its-counterparts-future-european-regulation>
- DATATYLSINET, **Artificial intelligence and privacy report**. Datatilsynet, 2018, p. 5, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>
- EDRI, **From 'trustworthy AI' to curtailing harmful uses: EDRI's impact on the proposed EU AI Act**, June 1 2021, <https://edri.org/our-work/from-trustworthy-ai-to-curtailing-harmful-uses-edris-impact-on-the-proposed-eu-ai-act/>
- EU4DIGITAL, **EU Digital Single Market**, <https://eufordigital.eu/discover-eu/eu-digital-single-market/>
- EUROPEAN COMMISSION, **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence**, 21/04/2021, COM/2021/205 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:205:FIN>
- EUROPEAN COMMISSION, **Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe**, Brussels, 25.4.2018 COM(2018) 237 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>
- EUROPEAN COMMISSION, **New rules for Artificial Intelligence – Questions and answers**, 21 April 2021, [https://ec.europa.eu/commission/presscorner/detail/en/QANDA\\_21\\_1683](https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683)
- EUROPEAN COMMISSION, **White paper on Artificial Intelligence - A European approach to excellence and trust**, Brussels, 19.2.2020 COM(2020) 65 final, [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf)
- EUROPEAN CONSUMER VOICE IN STANDARDISATION (ANEC), **ANEC comments on the European Commission proposal for an Artificial Intelligence Act**. Position Paper. July 2021. <https://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2021-G-071.pdf>
- EUROPEAN DATA PROTECTION BOARD AND EUROPEAN DATA PROTECTION SUPERVISOR, **Joint opinion 5/2021 on the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)**, 18 June 2021, [https://edpb.europa.eu/our-work-tools/our-documents/edpbbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpbbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en)

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, **Facial recognition technology: fundamental rights considerations in the context of law enforcement**. Publication Office of the European Union, 2019

GALLAND, Jean-Pierre, **The difficulties of regulating markets and risks in Europe through notified bodies**, European Journal of Risk Regulation, vol. 4, n. 3, 2013, pp. 365-373, p. 369, DOI: <https://doi.org/10.1017/S1867299X00002634>

GAUMOND, Eve, **Artificial Intelligence Act: What is the European approach for AI?**, June 4, 2021, Lawfare, <https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai>

GELLERT, Raphaël, **The risk- based approach to data protection**. Oxford University Press, 2020

GRIFFIN, Andrew, **Stephen Hawking: Artificial intelligence could wipe out humanity when it gets too clever as humans will be like ants**, Independent, 8 October 2015, <https://www.independent.co.uk/life-style/gadgets-and-tech/news/stephen-hawking-artificial-intelligence-could-wipe-out-humanity-when-it-gets-too-clever-humans-could-become-ants-being-stepped-a6686496.html>

IRISH DATA PROTECTION COMMISSION, **Taking photos at school events – Where common sense comes into play**, 12th April 2019, <https://www.dataprotection.ie/en/dpc-guidance/blogs/taking-photos-school-events-where-common-sense-comes-play>

LAUGHLIN, Andrew, **Which? Warns parents not to use a security camera as a baby monitor**, 24 Jul 2020, <https://www.which.co.uk/news/2020/07/which-warns-parents-not-to-use-a-security-camera-as-a-baby-monitor/>

LI, Daitian, TONG, Tony W., XIAO, Yangao, **Is China emerging as the global leader in AI?**, Harvard Business Review, February 18, 2021, <https://hbr.org/2021/02/is-china-emerging-as-the-global-leader-in-ai>

MENECEUR, Yannick, **European Commission's Alregulation proposal: betweentoo much and too little?**, April 23, 2021, <https://www.linkedin.com/pulse/european-commissions-ai-regulation-proposal-between-too-meneceur/>

PARLAMENTO EUROPEU E CONSELHO, **Decisão n. 768/2008/CE do Parlamento Europeu e do Conselho, de 9 Julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE**, <https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32008D0768>

PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à disputabilidade e equidade dos mercados no sector digital (Regulamento Mercados Digitais)**, Bruxelas, 15.12.2020, COM(2020) 842 final, 2020/0374(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados)**, Bruxelas, 25.11.2020, COM(2020) 767 final, 2020/0340(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0767&from=EN>

PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais (Regulamento Serviços Digitais) e que altera a Directiva 2000/31/CE**, Bruxelas, 15.12.2020, COM(2020) 825 final, 2020/0361(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0825&from=en>

PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às máquinas e seus componentes e acessórios**, Bruxelas, 21.4.2021, COM(2021) 202 final, 2021/0105(COD), <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0202&from=EN>



PARLAMENTO EUROPEU E CONSELHO, **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento inteligência artificial) e altera determinados actos legislativos da união**, 21/04/2021, COM/2021/206 final, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>

PARLAMENTO EUROPEU, **Resolução do Parlamento Europeu, de 20 de Outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial (2020/2014(INL))**, [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_PT.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PT.pdf)

PIPER, Kelsey, **Why Elon Musk fears artificial intelligence**, Vox, Nov 2, 2018, <https://www.vox.com/future-perfect/2018/11/2/18053418/elon-musk-artificial-intelligence-google-deepmind-openai>

RAPOSO, Vera Lúcia. **May I Have Some Artificial Intelligence with My Human Rights? About the Recent European Commission's Proposal on a Regulation for Artificial Intelligence**, KSLR EU Law Blog, May 24 2021. Retrieved 12 June 2021, <https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1569>

SIEMENS, **EU's AI Regulation proposal (21/04/2021) Position & recommendations**, July 2021, [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662941\\_en?fbclid=IwAR1W6QQXqsZgrCkZM5Z9W22JVFg0RDrh-gc4dFIXvg8z-z-fAhAQi66y39Y](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662941_en?fbclid=IwAR1W6QQXqsZgrCkZM5Z9W22JVFg0RDrh-gc4dFIXvg8z-z-fAhAQi66y39Y)

SKELTON, Sebastian Klovig, **Europe's proposed artificial intelligence regulation falls short on protecting rights**, computerweekly.com, 22-28 June 2021, <https://www.computerweekly.com/feature/Europes-proposed-AI-regulation-falls-short-on-protecting-rights>

SWEDSOFT, **Comments Regarding the European Commission's proposal for an Artificial Intelligence Act**, 24 June 2021, <https://www.regeringen.se/49eb04/contentassets/59dff9749d5e4cfa8d51146dd026ff62/swedsoft.pdf>

VEALE, Michael, BORGESIU, Frederik, **Demystifying the draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach**, Computer Law Review International, vol. 22, no. 4, 2021, pp. 97-112. <https://doi.org/10.9785/cri-2021-220402>

---

# E-Judiciário e automação: freios e avanços na experiência brasileira

*Maria Cláudia Cachapuz<sup>62</sup>  
Maria Luiza Kurban Jobim<sup>63</sup>  
Silvia Levenfus<sup>64</sup>*

## RESUMO

O presente artigo tem por objeto a análise dos meios digitais disponibilizados nas unidades integrantes do Poder Judiciário, em especial do Tribunal de Justiça do Rio Grande do Sul (TJRS), para aferição da sua real efetividade na facilitação do acesso à justiça. A partir de metodologia exploratória, descritiva e dedutiva relacionada à temática, a cidadania digital é contextualizada como condição da autodeterminação informativa no e-Judiciário, nas duas grandes partes do estudo. Apostando em método empírico de pesquisa, por estudo de caso do TJRS, a concretização das recomendações e resoluções do CNJ é demonstrada, bem como o alinhamento com as demais ações promovidas pelas instituições públicas de acesso à Justiça em nome de maior inclusão, facilitação e qualificação dos serviços ofertados à sociedade.

## PALAVRAS-CHAVE

privacidade; proteção de dados; acesso à justiça; cidadania digital.

---

<sup>62</sup> Magistrada do TJRS. Doutora em Direito pela UFRGS. Professora de Direito Privado da UFRGS e da Feevale. E-mail: [mcmcachapuz@tjrs.jus.br](mailto:mcmcachapuz@tjrs.jus.br)

<sup>63</sup> Formada em Direito pela UFRGS. Mestrado (LLM) pela University of Kent. Advogada. E-mail: [luizajobim@gmail.com](mailto:luizajobim@gmail.com)

<sup>64</sup> Mestranda em Direito Privado junto à UFRGS. Formada em Direito na Fundação Escola Superior do Ministério Público (FMP). E-mail: [silvialevenfus@gmail.com](mailto:silvialevenfus@gmail.com)



---

# E-Judiciary and automation: brakes and advances in the Brazilian experience

*Maria Cláudia Cachapuz  
Maria Luiza Kurban Jobim  
Sílvia Levenfus*

## ABSTRACT

The present article draws on the analysis of the digital channels made available throughout the units of the Judiciary, with a special focus on the Tribunal de Justiça do Rio Grande do Sul (TJRS) to evaluate the real enhancement of the access to justice. Departing from a deductive and exploratory methodology, the intent is to contextualize the digital citizenship under the light of informational self-determination in the e-Judiciary. Based on an empirical research methodology and relying on the case study of the TJRS, the CNJ resolutions acquire effectiveness and additionally, demonstrate the alignment with other actions promoted by public institutions in their respective areas of scope aiming at greater inclusion, facilitation and enhancement of services provided to society.

## KEYWORDS

privacy, data protection, access to justice, digital citizenship.

## Introdução

No atual estágio de desenvolvimento da sociedade da informação<sup>65</sup>, não chega a ser surpresa observar-se a facilidade do aplicador do Direito de, por meio de um trabalho hermenêutico coordenado, tornar mais flexível a interpretação dos institutos jurídicos, de forma a fazê-la acompanhar a fluidez típica do uso das tecnologias para a efetivação de direitos constitucionalmente consagrados. Isso reflete, em parte, o mesmo assombro de Habermas quando lança o debate quanto à possibilidade de alcance de distintas “margens de decisão”<sup>66</sup> para a tomada de resoluções concretas na vida de relação – o que permite, guardadas as proporções, a constatação da existência de caminhos institucionais distintos para o estabelecimento normativo de freios às liberdades de avanço tecnológico. Conforme o autor, ou decide-se de forma autônoma, “segundo considerações normativas que se inserem na formação democrática da vontade”<sup>67</sup>, ou resulta-se, noutra margem, sujeito à arbitrariedade de soluções utilitaristas, “em função de preferências subjetivas, que serão satisfeitas pelo mercado”<sup>68</sup>.

Tradicionalmente, na Constituição Federal, o conceito de cidadania figura como fundamento da República Federativa do Brasil (art. 1º, II, CF). Na origem, tal conceito - concebido, *a priori*, com maior tônica à sua dimensão estática (NASCIMENTO; MORAIS, 2007) - espelha a íntima conexão com a ideia de soberania (art. 1º, I, CF), traduzindo-se numa relação direta à noção de território e de exercício de direitos fundamentais no âmbito da atuação de ingerência política do Estado nacional. O termo “cidadania” é ainda relacionado ao agir coletivo de quem, tanto contribui para a elaboração do estatuto normativo do sistema jurídico, como participa do exercício efetivo de liberdades no âmbito de um Estado democrático de Direito. Portanto, pelo seu exercício, a ideia de cidadania atinge, da mesma forma, um caráter dinâmico de realização, não se traduzindo como mero status de representação política no âmbito da soberania do país.

Daí porque a própria noção de cidadania, nessa dupla dimensão compreendida, não permite uma banalização ou flexibilização<sup>69</sup> do conteúdo jurídico que resta pressuposto no seu conceito, sob pena de correr-se o risco de experimentação empírica do que muitos autores apontam como um totalitarismo transumanista<sup>70</sup> na contemporaneidade. É justamente a ideia de 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 racional da lei dos homens para o exercício de liberdades essenciais ao funcionamento de um efetivo Estado democrático (ARENDR, 2004, p. 66).

---

<sup>65</sup> Sobre o assunto, ver: SCHWAB, Klaus. *A quarta revolução industrial*. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016. CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. Trad: Roneide Venancio Majer. v. 1. São Paulo: Paz e Terra, 2013.

<sup>66</sup> HABERMAS, Jürgen. *O futuro da natureza humana*. São Paulo, Martins Fontes, 2004, p. 18.

<sup>67</sup> HABERMAS, Jürgen. *O futuro da natureza humana*. São Paulo, Martins Fontes, 2004, p. 18.

<sup>68</sup> HABERMAS, Jürgen. *O futuro da natureza humana*. São Paulo, Martins Fontes, 2004, p. 18.

<sup>69</sup> Não se olvida a atribuição do termo para outras espécies jurídicas, a que se questiona inclusive a natureza jurídica. Ver sobre a concessão de cidadania a robô humanoide dotado de inteligência artificial em: HANSON ROBOTICS. Hi, I am Sophia. [S.l.], [s.d.]. Disponível em: <https://www.hansonrobotics.com/sophia/>.

<sup>70</sup> No tema, a doutrina de FERRY, L. *A revolução transumanista*. Barueri, Manole, 2018; FUKUYAMA, F. *Nosso futuro pós-humano*. Rio de Janeiro, Rocco, 2003; SANDEL, M. *Contra a perfeição*. Rio de Janeiro, Civilização Brasileira, 2013.

Ademais, não há como negar que a força normativa da Constituição está umbilicalmente ligada à ideia de justiça que a inspira: “Sentir juridicamente é implicar-se com o Direito vigente, com o todo ou com parte dele, dando-lhe apoio.” (VERDÚ, 2004, p. 53) Se há relação direta de proporcionalidade entre cidadania e Justiça - e os meios pelos quais tanto uma quanto a outra são exercitadas por meio de implemento de determinadas tecnologias no mundo digital -, a efetivação de canais concretos para o exercício da cidadania por meio do acesso ao Poder Judiciário é um caminho viável, mas complexo o suficiente para que não se torne banal<sup>71</sup>. A inclusão digital nunca pode ser uma definição meramente formal, senão que uma pauta de conteúdo.

Assim como a noção de cidadania adquire conteúdo amplo em razão da diversidade de territórios e meios (físicos e digitais) cuja transformação foi severamente acentuada para o mundo digital pela pandemia da COVID-19, também a ideia de Justiça apresenta mesma complexidade. Na medida em que um conceito de Justiça não pode ser traduzido, unicamente, como um pressuposto de exercício de jurisdição, também o Poder Judiciário, como primeiro representante de sua efetiva concretização, compromete-se, ativamente, com as transformações essenciais da sociedade, viabilizando que cidadãos tenham voz e construam pontes reais entre a particularidade dos casos, em que identificados conflitos de liberdades e de exercício de posições de igualdade jurídica, e a universalidade exigida em abstrato pela aplicação da norma. Por isso, apostando-se ainda em método empírico de pesquisa, por estudo de caso, analisa-se, por meio de abordagem dedutiva, se o modelo de estudo para um e-Judiciário, ao lado de um e-cidadão – aqui, pressupondo-se essa complexidade do mundo digital -, está hoje transcrito em normas de conduta e de realização institucional de Justiça tanto na normatividade do CNJ, quanto, pragmaticamente, na disciplina normativa do Poder Judiciário gaúcho.

A partir de uma metodologia exploratória, descritiva e dedutiva, é objeto do presente artigo adentrar na relação estabelecida entre cidadania e realização de justiça, autodeterminação informativa e exercício de direitos fundamentais, de forma a compreender em que medida preserva e realiza, efetivamente, o Estado democrático de Direito por meio da adoção de políticas públicas de acesso digital. Quer-se, dessa forma, buscar responder se há hoje suficiência normativa para responder aos desafios propostos pelos avanços tecnológicos, especialmente na análise das questões que afetam direitos de personalidade, sem se furtar à discussão quanto ao aparente conflito de tal realidade frente às necessidades de maior inclusão e acesso à Justiça em termos digitais.

---

<sup>71</sup>A ideia pressuposta de banalidade é a mesma trabalhada por Hannah Arendt em *Eichmann em Jerusalém. Um relato sobre a banalidade do mal*, São Paulo, Companhia das Letras, 1999.

## 1. Cidadania Digital

Na era atual da sociedade da informação<sup>72</sup>, cujo processo de digitalização foi severamente acelerado pelas medidas de contenção à pandemia da COVID-19 a preocupação com a construção de Poder Público mais conectado – e responsivo – às necessidades os cidadãos é um anseio também do Poder Judiciário. A mudança drástica de comportamento, em certa medida, acelera a implantação da normatividade tanto da proteção quanto da segurança de dados, exigindo adaptações instantâneas, principalmente no âmbito público.

A seguir, apresentar-se-á de que forma vem se dando o implemento de uma cidadania digital (*e-cidadania*) e, em que medida, reflete em iniciativas do Poder Judiciário, influenciando a criação de novo termo, qual seja, *e-Judiciário*.

### 1.1 e-Cidadania

Dentro dessa sistemática, no ano de 2020, inaugura-se um novo marco legislativo no Brasil. Entra em vigor, em sua maior parte, uma das maiores salvaguardas à efetiva proteção dos usuários de serviços públicos, titulares de dados pessoais, qual seja, a Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

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. Permite-se, assim, observar uma interação, no espaço digital, cada vez mais fluida entre os espaços destinados ao que é público e privado<sup>73</sup>, tornando cada vez menos identificável a necessária distinção entre eles<sup>74</sup>. Ainda que muitos dos princípios e diretrizes gerais da LGPD pudessem ser extraídos de uma interpretação sistemática de comandos constitucionais sobre diplomas legais diversos<sup>75</sup>, 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 envolvidos no tratamento de dados pessoais, inclusive àqueles investidos em ações de finalidade pública.

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 permitir maior aperfeiçoamento das políticas públicas baseadas em evidências, diminuindo os custos de transação respectivos a ambos os

---

<sup>72</sup> O conceito de privacidade – ressignificado em virtude dos adventos tecnológicos –, é o “direito de manter o controle sobre as próprias informações” (RODOTÁ, 2008, p. 92), e não mais o clássico “direito de permanecer só”, referido pelo Juiz Cooley e mencionado na doutrina de Samuel Warren e Louis Brandeis em *The Right to Privacy*. Harvard Law Review, vol. 4, n. 5, p.193-220, dez. 1890.

<sup>73</sup> Sobre a temática, ver: CACHAPUZ, Maria Cláudia. *A obrigação pelo discurso jurídico: argumentação em temas de Direito Privado*. Sergio Antonio Fabris Editor: Porto Alegre, 2018, p. 31- 47.

<sup>74</sup> 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*.

<sup>75</sup> Sobre a matéria de normativas setoriais de proteção de dados anterior à LGPD, bem como o histórico de construção da referida lei ver: DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da Nova Lei Geral de Proteção de Dados brasileira. In: CAVALLI, Olga; BELLI, Luca. *Governança e regulações da internet na América Latina*. p. 309 – 325, 2019. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/27164>. Acesso em: 18 jun. 2021.

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). O norte cidadão é também incorporado nos dizeres da própria LGPD, art. 1º, *in fine*, na medida em que menciona dentre outros objetivos, 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<sup>76</sup> pelas pessoas (art. 2º, VII, *in fine*, LGPD), 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.

Adicionalmente, foi publicada, em 29 de março de 2021, a Lei nº 14.129<sup>77</sup>, a qual dispõe sobre os princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, especialmente por meio da desburocratização, da inovação, da transformação digital e da participação do cidadão. A dita normativa vem ao encontro de parâmetros estabelecidos também no prisma internacional. O referido diploma estabelece como princípios básicos e diretrizes, nos termos do seu art. 3º:

- i. a desburocratização, a modernização, o fortalecimento e a simplificação da relação do poder público com a sociedade, mediante serviços digitais, acessíveis inclusive por dispositivos móveis;
- ii. a disponibilização em plataforma única do acesso às informações e aos serviços públicos, observadas as restrições legalmente previstas e sem prejuízo, quando indispensável, da prestação de caráter presencial;
- iii. a possibilidade aos cidadãos, às pessoas jurídicas e aos outros entes públicos de demandar e de acessar serviços públicos por meio digital, sem necessidade de solicitação presencial;
- iv. a transparência na execução dos serviços públicos e o monitoramento da qualidade desses serviços;
- v. o incentivo à participação social no controle e na fiscalização da administração pública;
- vi. o dever do gestor público de prestar contas diretamente à população sobre a gestão dos recursos públicos;
- vii. o uso de linguagem clara e compreensível a qualquer cidadão;
- viii. o uso da tecnologia para otimizar processos de trabalho da administração pública;
- ix. a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de dados pessoais em ambiente

---

<sup>76</sup> 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). Quanto aos efeitos nefastos da falta de civilidade e da limitação às liberdades, disserta Fromm, no âmbito da psique-social, o seu papel na insurreição de Estados totalitários. (FROMM, 1974).

<sup>77</sup> Ver na íntegra: <https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132>

seguro quando for indispensável para a prestação do serviço, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e, quando couber, com a transferência de sigilo, nos termos do art. 198 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e da Lei Complementar nº 105, de 10 de janeiro de 2001;

- x. a simplificação dos procedimentos de solicitação, oferta e acompanhamento dos serviços públicos, com foco na universalização do acesso e no autosserviço;
- xi. a eliminação de formalidades e de exigências cujo custo econômico ou social seja superior ao risco envolvido;
- xii. a imposição imediata e de uma única vez ao interessado das exigências necessárias à prestação dos serviços públicos, justificada exigência posterior apenas em caso de dúvida superveniente;
- xiii. a vedação de exigência de prova de fato já comprovado pela apresentação de documento ou de informação válida;
- xiv. a interoperabilidade de sistemas e a promoção de dados abertos;
- xv. a presunção de boa-fé do usuário dos serviços públicos;
- xvi. a permanência da possibilidade de atendimento presencial, de acordo com as características, a relevância e o público-alvo do serviço;
- xvii. a proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
- xviii. o cumprimento de compromissos e de padrões de qualidade divulgados na Carta de Serviços ao Usuário;
- xix. a acessibilidade da pessoa com deficiência ou com mobilidade reduzida, nos termos da Lei nº 13.146, de 6 de julho de 2015 (Estatuto da Pessoa com Deficiência);
- xx. o estímulo a ações educativas para qualificação dos servidores públicos para o uso das tecnologias digitais e para a inclusão digital da população;
- xxi. o técnico aos entes federados para implantação e adoção de estratégias que visem à transformação digital da administração pública;
- xxii. o estímulo ao uso das assinaturas eletrônicas nas interações e nas comunicações entre órgãos públicos e entre estes e os cidadãos;
- xxiii. a implantação do governo como plataforma e a promoção do uso de dados, preferencialmente anonimizados, por pessoas físicas e jurídicas de diferentes setores da sociedade, resguardado o disposto nos arts. 7º e 11 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), com vistas, especialmente, à formulação de políticas públicas, de pesquisas científicas, de geração de negócios e de controle social;
- xxiv. o tratamento adequado a idosos, nos termos da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);
- xxv. a adoção preferencial, no uso da internet e de suas aplicações, de tecnologias, de padrões e de formatos abertos e livres, conforme disposto no inciso V do caput do art. 24 e no art. 25 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet); e
- xxvi. a promoção do desenvolvimento tecnológico e da inovação no setor público. (grifos acrescidos).

Depreende-se, pois, que 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, questões igualmente relevantes.

## 1.2 E-Judiciário: o CNJ, o TJRS e os canais digitais no mundo digital

A busca pela cidadania digital, bem como por um Judiciário mais moderno, por parte do CNJ, não é recente<sup>78</sup>. Entretanto, somente no ano de 2020, é que se tornaram mais recorrentes os esforços para orientar, por meio de publicações administrativas, a adoção de medidas específicas e tecnológicas pelos tribunais brasileiros. Em parte, em virtude da necessária aceleração virtual causada pela pandemia da COVID-19, em parte pela atualização e modernização de sistemas e da inteligência artificial, bem como da entrada em vigor da LGPD. Nessa enseja, impende destacar algumas publicações do CNJ, especificamente, selecionadas<sup>79</sup> para fins de possibilitar um cotejo no campo pragmático com as atividades levadas a cabo pelo Judiciário gaúcho.

Quanto à implementação da LGPD no âmbito dos tribunais, foi publicada a Recomendação nº 73/2020<sup>80</sup>, de agosto de 2020, e também criado grupo trabalho, no CNJ, responsável por elaborar discussões a respeito da matéria e trabalhar na formulação das prescrições específicas quanto ao tema, a partir da Portaria nº 212/2020<sup>81</sup>, datada de outubro de 2020. Ainda, publicada a Resolução nº 363/2021<sup>82</sup>, de janeiro de 2021, que visa a implementação de medidas pelos tribunais para a adequação à LGPD. Por sua vez, o TJRS, desde maio de 2020, instaurou 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 no âmbito administrativo da Corte. A criação de uma comissão de estudos específica para a implementação da LGPD no âmbito do TJRS foi formalizada (Ato nº 027/2020<sup>83</sup>), em junho de 2020, publicando-se, na sequência, portarias de nomeação de seus respectivos membros (058, 068/2020 e 112/2020). Posteriormente, foi

---

<sup>78</sup> Exemplifica-se com: <https://www.cnj.jus.br/modernizacao-do-judiciario-e-tema-do-congresso-da-cidadania-digital/>

<sup>79</sup> Outras resoluções que neste estudo não serão abordadas, mas cabe a menção: Resolução nº 372/2021 (Balcão Virtual), destaca-se que, desde março de 2021, o Tribunal gaúcho conta com o Balcão Virtual em funcionamento. O novo canal de atendimento do Judiciário se dá por meio de videoconferência, sendo possível o contato imediato com cada unidade judiciária; Resolução nº 345/2020 (CNJ), sobre o "Juízo 100% Digital". Em um dos considerandos, há a referência de que é incumbência do Poder Judiciário a implantação de mecanismos para efetivar o amplo acesso à Justiça. Ainda, dentre as disposições, destaca-se a faculdade de escolha do "Juízo 100% Digital" quando da distribuição da ação, bem como, por iniciativa do magistrado, a manifestação, a qualquer momento, das partes sobre a adoção do "Juízo 100% Digital". Inclusive, a publicação de Cartilha (ver em [https://www.cnj.jus.br/wp-content/uploads/2020/10/WEB\\_cartilha\\_Juizo\\_100porcento\\_digital\\_v3.pdf](https://www.cnj.jus.br/wp-content/uploads/2020/10/WEB_cartilha_Juizo_100porcento_digital_v3.pdf)) sobre o tema corrobora para que os jurisdicionados tenham ciência do projeto, bem como compreendam os esforços por parte do Poder Judiciário para tornar acessível a jurisdição, não somente em âmbito físico.

<sup>80</sup> Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Ver na íntegra: <https://atos.cnj.jus.br/atos/detalhar/3432>

<sup>81</sup> Institui Grupo de Trabalho destinado à elaboração de estudos e de propostas votadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências. Ver na íntegra: <https://atos.cnj.jus.br/atos/detalhar/3520>

<sup>82</sup> Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Ver na íntegra: <https://atos.cnj.jus.br/atos/detalhar/3668>

<sup>83</sup> Ver o documento na íntegra: <https://www.tjrs.jus.br/static/2020/07/Ato-n%C2%BA-027-2020-P-2.pdf>



nomeado o encarregado da proteção de dados pessoais (Portaria nº 094/2020-P<sup>84</sup>), para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Para se interpretar e se aplicar 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<sup>85</sup>.

A partir dessas premissas, o TJRS estabeleceu, no art. 2º do Ato nº 037/2020, a garantia, 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), de *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*<sup>86</sup>) - 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.

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*<sup>87</sup> - 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*.

Nesse sentido, não menos importante é a atenção para com a criação de meios efetivos de instrumentalização do direito de acesso pelos titulares. A estruturação de um formulário eletrônico para exercício dos direitos do titular em sítio eletrônico próprio deve, por um lado, se preocupar com a necessária autenticação e conferência

---

<sup>84</sup> Ver o documento na íntegra :<https://www.tjrs.jus.br/static/2020/10/Portaria-094-2020-P-1.pdf>

<sup>85</sup> Íntegra do ato disponível em: <https://www.tjrs.jus.br/static/2020/09/Ato-037-2020-P-LGPD.pdf>

<sup>86</sup> "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/privacyright*), 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.

<sup>87</sup> Sobre o tema, ver a doutrina de: CAVOUKIAN, Ann. *Privacy by design – The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario. Publicado originalmente em agosto de 2009. Revisado em janeiro de 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 14 abr. 2021.



da identidade do requerente e, de outro, com a facilitação do acesso e agilidade no seu atendimento.

As sistemáticas adotadas e em implementação em relação à LGPD dizem, de forma conexa, para com a prevenção de potenciais problemas a serem enfrentados e com a criação preliminar de salvaguardas a serem erigidas em processos automatizados na esfera institucional – seja no âmbito administrativo, seja no judicial. Isto porque a Resolução nº 332/2020<sup>88</sup>, que permeia orientações sobre a adoção da Inteligência Artificial (IA) no Poder Judiciário, preconiza a saudável coexistência entre o algoritmo e o humano, com observância aos Direitos Fundamentais, a critérios éticos de transparência, à previsibilidade, à auditoria, à garantia de imparcialidade, à justiça substancial, à igualdade e à não discriminação. O desiderato é, pois, possibilitar o desenvolvimento de IA que promova o bem-estar dos cidadãos e a prestação não somente de uma jurisdição equitativa (CNJ, 2020), mas também de uma justiça acessível por diferentes meios e através de diferentes portas.

Apesar de a inteligência artificial<sup>89</sup> entrar no campo do Direito com função auxiliar – e não substitutiva – aos operadores, a capacidade de que tal processo venha a interferir de forma discriminatória, antiética ou errônea nos processos decisórios administrativos e judiciais é inegável. A definição ampla do que se entende como IA, nos termos da própria Resolução do CNJ nº 332/2020, como qualquer conjunto de dados e algoritmos concebidos a partir de modelos matemáticos<sup>90</sup>, 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. A utilização desta tecnologia pode gerar vieses discriminatórios, seja pela ausência de revisão dos algoritmos ou banco de dados munido de informações insuficientes para a matéria que se propõe realizar<sup>91</sup>. Como a tecnologia pode vir a acentuar abismos estruturais e discriminatórios na sociedade, cabe modulá-la para que venha a minimizá-los, a partir do uso que se faz dela, e não a acentuá-los.

---

<sup>88</sup> Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. (CNJ, 2020). Ver na íntegra: <https://atos.cnj.jus.br/atos/detalhar/3429>

<sup>89</sup> Para aprofundamento da matéria sobre inteligência artificial: EUROPA, Parlamento Europeu. *Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica*. (2015/2103 (INL)). Brussels: Parlamento Europeu, 2017. Disponível em: [http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051\\_PT.html?redirect#title2](http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html?redirect#title2). Acesso em: 27 mar. 2021; EUROPEAN COMMISSION. *A definition of AI: Main Capabilities and disciplines*. Brussels, 2019. P. 1-9, p. 6. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em 20 mar. 2021; BUCHANAN, Bruce. A (very) brief history of artificial intelligence. *AI Magazine*, v. 26, n.6, p.53-60, 2005; DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto Nuno Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Revista de Ciências Jurídicas*, v.23, p.1-17, 2018.

<sup>90</sup> 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”.

<sup>91</sup> Exemplifica-se com: WASHINGTON, Anne L. How To argue with na algorithm: lessons from the COMPAS-Propublica debate. *The Colorado Technology Law Journal*. v. 17, p. 1-37, 2019. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3357874](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3357874). Acesso em: 09 abr. 2021; BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research* 81. Conference on Fairness, Accountability, and Transparency, 2018. P. 1-15. Disponível em: <http://proceedings.mlr.press/v81/boulamwini18a/boulamwini18a.pdf>. Acesso em: 13 mar. 2021; NIST. *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 13. mar, 2021

Nesse sentido, e diante dos desafios a serem perpassados, a IA, no âmbito do TJRS, vem sendo testada, desde o final de 2019, na Comarca de Tramandaí, em processos de executivos fiscais no *e-proc*<sup>92</sup>. O objetivo principal é, após a distribuição do processo, auxiliar na classificação do despacho a ser proferido. Com esta ferramenta, visa-se justamente à diminuição do tempo despendido em atividade mecânica. O fato, porém, não desautoriza o poder do Magistrado ao qual o processo é vinculado para fins de conferir a adequação da sugestão trazida – ou não a seguir, caso prefira. No âmbito recursal, a IA vem sendo utilizada para fins de catalogação de processos e distribuição de competências entre as câmaras integrantes. Após a sugestão trazida automaticamente no sistema *e-proc*, servidores responsáveis pela distribuição dos processos confirmam a adequação, ou não, do encaminhamento dado previamente.

Sob perspectiva diversa, a ideia de que a Justiça não se encontra unicamente na jurisdição, mas também nos métodos consensuais para solução de conflitos regrada, no âmbito do CNJ, pela Resolução nº 125/2010, é plenamente aplicável ao pano de fundo, da cidadania digital, relacionado ao presente estudo. Dentro dessa sistemática, também a noção de exercício de direitos deve ser horizontalizada nas portas ofertadas pelas unidades judiciais. Como já referido pelo Min. Ricardo Villas Bôas Cuevas em recente entrevista, “uma justiça multiportas (...) deve oferecer a todos os cidadãos uma solução justa para seus problemas e (...) não necessariamente passa por demandas judiciais<sup>93</sup>”.

No âmbito conceitual, a Justiça Multiportas preconizada pelo CNJ significa viabilizar ao cidadão o encontro de informações sobre os serviços da justiça de que necessita, além de como pode usufruí-los. É possível não somente obter informações acerca de questões judiciais, mas também de modalidades de solução de conflitos de forma extrajudicial. Nesse sentido, até mesmo o espírito de uma Justiça Multiportas é redimensionado para o âmbito administrativo do TJRS. Isto porque as atividades realizadas pelo Poder Judiciário podem ser acionadas, conferidas, fiscalizadas, monitoradas ou mesmo questionadas através de canais de acesso específicos diversos, desde a Central de Atendimento ao Cidadão (SAC) até as Ouvidorias, desde denúncias quanto à integridade da instituição e de seus agentes até o monitoramento do tratamento dos dados pessoais dos titulares pela instituição.

Dessa forma, cada vez mais canais de acesso para fruição de serviços administrativos buscam ser simplificados para fins de facilitar o seu uso e encontro por aqueles que os buscam e dar efetividade ao exercício da cidadania. Dentro dessa estrutura ainda em formação, o TJRS trabalha, nesse sentido, na reestruturação de seus canais digitais de interação com o público, na elaboração de ferramenta que, em percurso intuitivo e de fácil acesso, faça com que não somente pedidos sejam recebidos, mas que também sejam procedimentalizados e respondidos com a maior celeridade possível.

Verifica-se, pois, que questões relacionadas ao mapeamento do fluxo de dados dentro dos tribunais é condição não somente de cumprimento de dever legal – e administrativo – dos órgãos judiciais, mas também de demonstração ao cidadão de que o retrato institucional de que dele emana, a partir da consolidação de todos os

---

<sup>92</sup>Ver: <https://www.tjrs.jus.br/novo/noticia/inteligencia-artificial-acelera-a-tramitacao-dos-processos-de-execucao-fiscal-e-aqiliza-a-cobranca-de-receita-pelos-entes-publicos/>; [Inteligência Artificial avança nos Executivos Fiscais Estaduais - Tribunal de Justiça - RS \(tjrs.jus.br\)](https://www.tjrs.jus.br/novo/noticia/inteligencia-artificial-avanca-nos-executivos-fiscais-estaduais-tribunal-de-justica-rs/)

<sup>93</sup><https://www.cnj.jus.br/justica-multiportas-oferece-caminhos-adequados-a-solucao-de-conflitos-em-mt/>

locais onde seus dados pessoais são tratados, é devidamente justificado, verídico, atual e adequado. Por outro lado, a rapidez, eficiência e celeridade nas respostas aos cidadãos (com prazo extremamente exíguos, como é aquele previsto pelo art. 19 da LGPD, ainda que sujeito a regulamentação ulterior), implica que soluções ágeis sejam crescentemente buscadas pelos setores públicos, em conjugação de esforços como setor privado, em sistemas informáticos abrangentes, unificados, interoperáveis e confiáveis com armazenamentos não mais somente em locais físicos, mas também em nuvem.

Apesar de não se pretender a substituição de julgadores por máquinas, o fato da IA atuar como auxiliar em processos decisórios, pode acabar tornando mais tênues essas diferenciações, o que exigirá a adoção de salvaguardas tecnológicas e jurídicas para a sua regular procedimentalização (ALMADA; DYMITRUK, 2021). Isso porque, “enquanto se convive com a possibilidade real de ultrapassagem da capacidade intelectual humana – leia-se, racionalidade – pelo desenvolvimento de uma racionalidade própria à IA, urge a necessidade de estabelecimento de garantias à inserção do controle humano nos processos decisórios e automatizados definidos por operações algorítmicas<sup>94</sup>” (CACHAPUZ, 2019).

Ademais, tanto na esfera jurisdicional quanto na administrativa, a sistematização de algoritmos deve vir pautada por critérios de transparência tanto na sua construção quanto no seu aprendizado de máquina. A composição dos grupos responsáveis por desenvolver a IA em sentido amplo, ao determinar a presença de grupos minoritários, tem, inclusive, a intenção de diminuir potenciais enviesamentos prejudiciais ou preconceituosos que venham a ser desenvolvidos em termos decisórios.

## 2. e-Justiça

Os esforços para transformar os ideais de uma e-Justiça em realidade é um trabalho diário do Poder Judiciário. Mas, para que tal seja possível, é essencial que estejam presentes as bases que fortificam e impulsionam a cidadania nessa instituição, quais sejam: (i) a autodeterminação informativa e (ii) a real incrementação do acesso a esses serviços.

### 2.1 Autodeterminação informativa

A ideia de qualidade da informação aparece, via de regra, como uma das condições de sustentação e proteção de uma esfera de privacidade<sup>95</sup> quando analisados modernos sistemas de interconexão de dados pessoais por bancos cadastrais. Como a ideia de autodeterminação informativa apropria-se de conceitos

---

<sup>94</sup> CACHAPUZ, Maria Cláudia. “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* n° 20, 2019, p. 63-86.

<sup>95</sup> Assim explica Ana Isabel Ortiz: “A ‘qualidade dos dados’ como princípio em que se baseia a legalidade da recolha e subsequente tratamento dos mesmos deve ser considerada numa dupla perspetiva: a ‘qualidade dos dados pessoais’ e a finalidade do tratamento. , os dados atingem uma determinada qualidade e o seu tratamento é lícito porque está relacionado com as finalidades legítimas que inspiram o tratamento. Então, os dados serão adequados quando estiverem diretamente relacionados com a finalidade específica, quando for necessário para o cumprimento de o mesmo.; Mas, por outro lado, também será adequado quando responder à veracidade e exatidão e integridade das informações relativas à pessoa e, finalmente, os dados não serão excessivos quando forem fornecidos no que diz respeito a referida finalidade, ou seja, os dados estritamente necessários ao seu cumprimento, e sua coleta não é abusiva ou desproporcional em relação à finalidade de cada tratamento” (ORTIZ, 2002, p. 211)

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 em um 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 (BVerfGE 65,1, 1983), pois exige a reciprocidade de conduta a quem se dispõe à liberação dos dados e a quem pretende obter determinado acesso<sup>96</sup>.

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<sup>97</sup>), 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 texto atual da LGPD brasileira, especialmente no trato dos bancos cadastrais públicos<sup>98</sup>.

Relembre-se que, a própria normativa protetiva de dados dispõe, em capítulo próprio (Capítulo III), dentre os direitos dos titulares, a possibilidade de obtenção do controlador, a qualquer momento e por meio, de requisição; da confirmação do tratamento de seus dados, bem como acesso aos dados que lhe dizem respeito e correção de dados incompletos, inexatos ou desatualizados, inclusive prevendo a possibilidade de revogar do consentimento anteriormente concedido<sup>99</sup>. Ademais, o próprio armazenamento dos dados pessoais deve ser promovido “em formato que favoreça o exercício do direito de acesso”<sup>100</sup>(BRASIL, 2020).

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. Terceiro, porque o paradigma de um Marco de Políticas Integradas para apoiar uma abordagem integral do governo que conduza à criação de políticas coerentes na era digital (OCDE, 2020) possui como três dos seus elementos fulcrais o acesso, o uso e a

---

<sup>96</sup> O debate iniciou-se em 1982, quando da contestação da Lei do Censo alemã (*Volkszählungsgesetz*), Ver: MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais*. Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016; SCHWABE, J. *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. MARTINS, Leonardo; HENNIG, Beatriz et al (trad). Uruguai: Konrad-Adenauer Stiftung – KAS 2005.

<sup>97</sup> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. (BRASIL, 2011).

<sup>98</sup> Vide Art. 5º, XVI e Art. 63 da LGPD

<sup>99</sup> Vide Art. 18, I, II, III e IX da LGPD

<sup>100</sup> Vide Art. 19, §1º da LGPD.

confiança dos canais digitais, o que pressupõe, em primeiro plano, a preservação da autodeterminação dos titulares na participação – e construção – de um espaço público aberto à comunicação e transparente em termos de processamento de informações.

## Acesso à e-Justiça

As atividades do Poder Judiciário devem ser compreendidas em sua acepção ampla, abarcando não somente a função jurisdicional, mas também administrativa. Não é sem razão, inclusive, que as ações iniciais relacionadas à necessária harmonização entre os preceitos da Lei de Acesso à Informação (LAI) e a LGPD foram iniciadas na sua atividade eminentemente administrativa. Dentro desse aspecto, estão os canais existentes e em implantação, relacionados aos (i) direitos de se obter informação, por parte dos cidadãos, dos órgãos públicos com base na LAI; (ii) direitos de acesso, como titulares de dados pessoais, com base na LGPD; (iii) direitos de participação, como capazes de contribuir, ativamente, na configuração e aprimoramento da instituição e dos respectivos serviços por meio da Ouvidoria e (iv) direitos de fiscalização, por meio do recebimento de denúncias relacionadas à integridade institucional que assegurem o *compliance* da atividade pública desempenhada pelo Poder Judiciário.

Percebe-se que, dentro dos canais digitais, dados são tanto o pressuposto como a matéria necessária à transformação digital e facilitação de acesso ao público que se busca salvaguardar. Consequentemente, a proteção aos dados pessoais dos indivíduos em uma sociedade informatizada, tanto como meio quanto fim não se restringe ao canal de acesso (ii) supratranscrito. É, pois, imprescindível ao titular de dados de que exerça a supervisão sobre a informação que lhe compete tanto em relação à demonstração conferida por um interesse público no armazenamento de dados, como 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<sup>101</sup> – de um amplo direito de acesso dos indivíduos às suas informações nominativas<sup>102</sup>, como inicialmente existente na Lei 8.078/90 (Código de

---

<sup>101</sup> 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, regando 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.

<sup>102</sup> 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



Defesa do Consumidor), impondo a comunicação de registro de dados pessoais do consumidor em cadastro de consumo e crédito. Traduzindo a sua interlocução para o plano público-administrativo foco do presente estudo, 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, diretriz esta também replicada na recente legislação sobre o Governo Digital (art. 3º, VII, da Lei nº 14.129/21<sup>103</sup>). 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<sup>104</sup> que atinge a realização plena de um conceito de autodeterminação informativa<sup>105</sup>. 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<sup>106</sup>.

Também se encontra relacionada a um direito mais amplo de acesso às informações nominativas do indivíduo - que se vejam registradas em banco cadastral - a 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. A preocupação real com a fonte e segurança de dados pessoais adquire, portanto, posição proeminente, de modo a viabilizar não apenas, em momento posterior, a interoperabilidade entre os sistemas públicos (art. 3º, XIV, da Lei nº 14.129/21), mas antes disso, da qualidade essencial - e veracidade - que lhes são pressupostas por meio da “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (art. 6º, V, da LGPD)<sup>107</sup>.

Rememorando a origem histórica e tomando como exemplo a normativa norte-americana sobre a matéria, encontra-se, ainda no PrivacyAct de 1974, a preocupação de que as agências de coleta e armazenamento de dados retenham

---

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 abrangem, cumulativamente, a possibilidade indenizatória em face de prejuízo demonstrado em concreto - situação inatingível por meio de um remédio constitucional.

<sup>103</sup> “Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública: [...], VII - o uso de linguagem clara e compreensível a qualquer cidadão”. (BRASIL, 2021).

<sup>104</sup> Esclarece Ana Ortiz, com enfoque à experiência espanhola de disciplina sobre a proteção de dados pessoais geridos por bancos cadastrais: “Sem a proclamação do princípio da publicidade, os direitos dos cidadãos pereceriam e padeceriam de uma grava quebra de sua efetividade e satisfação” (tradução livre). (ORTIZ, 1998, p. 247).

<sup>105</sup> 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.

<sup>106</sup> Os direitos dos titulares estão previstos no Capítulo III da LGPD (Arts. 17-22).

<sup>107</sup> 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. 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.

apenas aquelas informações que se tornem relevantes e que justifiquem o próprio cadastramento<sup>108</sup>. 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 InformationInfrastructureTask 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 para as finalidades que justificam sua coleta e utilização”<sup>109</sup>. Nada diferente do que reconhece, mais recentemente, o artigo 9º da LGPD brasileira.

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.

Percebe-se, portanto que o acesso à Justiça não se restringe ao acesso à jurisdição propriamente dita, uma vez que, questões preliminares, pretensamente periféricas, com o armazenamento de dados pessoais em bancos públicos têm o condão de influenciar, ativamente, em decisões ulteriores tanto na esfera administrativa própria do órgão, como também por agentes públicos ou privados que com base nelas perfilam os titulares.

Em período recente, em março de 2021, foi publicada a Estratégia Nacional de Inteligência Artificial, elaborada pelo Ministério de Ciência, Tecnologia e Inovação (MCTI), contendo as ações do governo federal para o desenvolvimento de soluções em IA por meio de seu “uso consciente, ético e em prol de um futuro melhor”. Conforme o dito guia, a IA representa, no campo do Poder Público, “importante oportunidade para melhorias na qualidade de atendimento e nos índices de satisfação dos cidadãos.” Isto porque, através da inovação na gestão dos serviços públicos, com a modernização dos processos administrativos, possibilita-se que o Estado, em seu sentido *lato*, “supere obstáculos burocráticos e restrições orçamentárias para oferecer serviços novos, melhores e mais eficientes à população.<sup>110</sup>” Se de um lado, o serviço da justiça requer facilitação e desburocratização, de outro, exige respeito ao indivíduo e segurança de suas informações.

Na medida em que dados públicos são fontes de informação consideradas inclusive superiores em termos de segurança<sup>111</sup>, e são utilizados como *inputs* de decisões algorítmicas nas mais variadas esferas e unidades, têm estes o condão de, assim, alterar

---

<sup>108</sup> Ainda na origem, pelo PrivacyAct, 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 necessária; (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, 1997, p. 77).

<sup>109</sup> 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 InformationInfrastructureTask Force).

<sup>110</sup> [https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia\\_estrategia.pdf](https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia.pdf)

<sup>111</sup> “CONSIDERANDO que os dados utilizados no processo de aprendizado de máquina deverão ser provenientes de fontes seguras, preferencialmente governamentais, passíveis de serem rastreados e auditados;” – Resolução 332/2020 CNJ

as oportunidades de vida dadas aos indivíduos. É como Solove aponta ser um dos grandes desafios da era atual: movermos da concepção de uma sociedade meramente Orwelliana para uma sociedade Kafkaniana. Aqui, 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 na metáfora de Kafka<sup>112</sup> –, 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.

Isto porque, se o retrato da pessoa digital, da e-pessoa<sup>113</sup>, construído a partir das autenticações necessárias para o acesso aos canais digitais é, por um lado, condição ao exercício da cidadania junto ao Poder Judiciário, deve ser somente utilizado em tratamentos posteriores compatíveis com a finalidade pelos quais determinados dados foram processados, com garantia da respectiva qualidade e veracidade que lhes são esperadas<sup>114</sup>, sob pena de graves fiscos de efeito bumerangue ao titular (NYB, 2021<sup>115</sup>) e de decréscimo da confiança dos cidadãos nos meios digitais que tanto se busca angariar<sup>116</sup>.

### 3. Conclusão

Abordar tema tão complexo como a cidadania em tempos tecnológicos requer muita cautela. Embora já enraizada beleza – aqui questionável – da adoção da e-Justiça, é preciso um olhar atento às suas consequências, sob pena de desenvolver papel contrário ao que se busca: facilitar o acesso, mas destituir as raízes mais puras do Direito.

A busca de uma implantação efetiva da e-cidadania deve ser pautada com cautela que se espera quando do tratamento de dados pessoais – aqui se inclui toda a sua abrangência e espectro. Isso porque, invocar a interface da cidadania e do acesso à justiça – elementos inerentes a uma sociedade democrática – com elementos ainda questionáveis, como a aplicação da inteligência artificial a processos, é um desafio.

Sabe-se que a dogmática – com inegável importância – não exerce papel sozinha neste meio. É preciso verificar se, de fato, os meios tecnológicos podem ser instituídos com pragmatismo. Assim, aplicar novas relações em tema tão complexo e fundamental, requer cuidado: para assegurar a autodeterminação informativa; para permitir um acesso à justiça virtual; para se estabelecer e permanecer uma relação de confiança entre Estado e cidadão. A tecnologia exige esse reforço.

---

<sup>112</sup> 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).

<sup>113</sup> Aqui não se está falando do termo *e-person*, cuja nomenclatura vem sendo utilizada em tentativa de encontrar uma natureza jurídica adequada ao robô. Nesse sentido, ver em: MARTINS-COSTA, Judith. Prefácio. In: CACHAPUZ, Maria Cláudia. *A obrigação pelo discurso jurídico. A argumentação em temas de Direito Privado*. Porto Alegre: Sergio Antonio Fabris editor, 2018. Antes disso, está-se falando da projeção da pessoa, como direito personalidade que é, no mundo digital. (SOLOVE, 2004).

<sup>114</sup> Aqui se pontua a preocupação com a utilização de técnicas biométricas – dados pessoais sensíveis; como o reconhecimento facial.

<sup>115</sup> <https://noyb.eu/en/right-access-data-protection-boomerang>

<sup>116</sup> Confiança esta baseada inclusive na guarda dos dados pessoais, mitigando a ocorrência de incidentes de segurança, como os vazamentos de dados.



De fato, em que pese haja hoje relativa suficiência normativa para responder aos primeiros desafios propostos pelos avanços tecnológicos, especialmente na análise das questões que afetam direitos de personalidade, não há como se afastar da discussão necessária que se impõe de enfrentamento do aparente conflito de tal realidade frente às necessidades de maior inclusão e acesso à Justiça em termos digitais. O estudo de caso, a partir de exemplos práticos levados a cabo pelo TJRS, por meio de metodologia exploratória descritiva, dedutiva e exploratória, de forma exemplificativa, demonstra não apenas uma tentativa efetiva de aplicação das recomendações e resoluções do CNJ na prática, como aponta, de forma clara, a oportunidade de promoções de ulteriores ações em nome de maior inclusão, facilitação e qualificação de serviços judiciais ofertados à sociedade.

É fato que ainda restam inúmeros debates a serem estabelecidos sobre a temática – principalmente na medida em que se apresentam desafios tecnológicos amplos para futuro -, mas espera-se ter contribuído, nessa pesquisa ainda embrionária, com tema tão essencial para a atualidade.

#### 4. Referências bibliográficas

ALMADA, Marco e DYMTRUK, Maria. Data Protection and Judicial Automation. In: *Research handbook on EU data protection*. Eleni Kosta and Ronald Leenes (eds.). Edward Elgar 2021, forthcoming.

BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research* 81. Conference on Fairness, Accountability, and Transparency, 2018. P. 1-15. Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 13 mar. 2021

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 13 abril 2021.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº93, de 26 de setembro de 2019. *Glossário de Segurança da Informação*. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 21 jul, 2020.

BRASIL. Lei nº 12. 527, de 18 de novembro de 2011. *Lei de Acesso à informação*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm). Acesso em 13 abr, 2021.

BRASIL. Lei nº13.709, 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em 28 nov. 2020

BRASIL. Lei nº 14.129, de 20 de março de 2021. *Lei do Governo Digital*. Disponível em: <https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132> Acesso em 25 mai 2020.

BUCHANAN, Bruce. A (very) brief history of artificial intelligence. *AI Magazine*, v. 26, n.6, p.53-60, 2005

CACHAPUZ, Maria Cláudia. 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*. Trad: Roneide Venancio Majer. v. 1. São Paulo: Paz e Terra, 2013.

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

CAVOUKIAN, Ann. **Privacy by design – The 7 Foundational Principles**. Information and Privacy Commissioner of Ontario. Publicado originalmente em agosto de 2009. Revisado em janeiro de 2011. Disponível em: <https://www.ipc.on.ca/wp->

[content/uploads/resources/7foundationalprinciples.pdf](#). Acesso em: 14 abr. 2021.

CNJ, Conselho Nacional Da Justiça. *CNJ usará automação e inteligência artificial para destravar execução fiscal*. Disponível em: <https://www.cnj.us.br/noticias/cnj/88740-cnj-usara-automacao-e-inteligencia-artificial-para-destravar-execucao-fiscal>. Acesso em: 31.07.2019

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da Nova Lei Geral de Proteção de Dados brasileira. In: CAVALLI, Olga; BELLI, Luca. *Governança e regulações da internet na América Latina*. p. 309 – 325, 2019. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/27164>. Acesso em: 18 jun. 2021.

DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de.; ANDRADE, Norberto Nuno Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Revista de Ciências Jurídicas*, v.23, p.1-17, 2018.

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

EUROPA. Parlamento Europeu. *Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica*. (2015/2103 (INL)). Brussels: Parlamento Europeu, 2017. Disponível em: [http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051\\_PT.html?redirect#title2](http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html?redirect#title2). Acesso em: 27 mar. 2021

EUROPEAN COMMISSION. *A definition of AI: Main Capabilities and disciplines*. Brussels, 2019. P. 1-9, p. 6. Disponível em: <https://ec.europa.eu/digital-singlemarket/en/news/definition-artificial-intelligence-main-capabilities-and-scientificdisciplines>. Acesso em 20 mar. 2021

FERRY, L. *A revolução transumanista*. Barueri, Manole, 2018.

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

FUKUYAMA, F. *Nosso futuro pós-humano*. Rio de Janeiro, Rocco, 2003.

HABERMAS, Jürgen. *O futuro da natureza humana*. São Paulo, Martins Fontes, 2004, p. 18.

HANSON ROBOTICS. Hi, I am Sophia. [S.l.], [s.d.]. Disponível em: <https://www.hansonrobotics.com/sophia/>

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

MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais*. Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016.

MARTINS-COSTA, Judith. Prefácio. In: CACHAPUZ, Maria Cláudia. *A obrigação pelo discurso jurídico. A argumentação em temas de Direito Privado*. Porto Alegre: Sergio Antonio Fabris editor, 2018.

NIST. *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 13. mar, 2021

NOYB. “*Right of Access as a data protection boomerang?*”. Disponível em: <https://noyb.eu/en/right-access-data-protection-boomerang>. Acesso em 25 mai. 2021.

OCDE (2020). *A caminho da Era Digital no Brasil*. Disponível em: <https://www.oecd.org/digital/a-caminho-da-era-digital-no-brasil-45a84b29-pt.htm>  
Acesso em: 26 mai 2021.

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

PORTARIA Nº 212/2020. Conselho Nacional de Justiça. Institui Grupo de Trabalho destinado à elaboração de estudos e de propostas votadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3520>. Acesso em: 31 mar, 2021.

RECOMENDAÇÃO Nº 73/2020. Conselho Nacional de Justiça. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3432>. Acesso em: 30 mar. 2021

RESOLUÇÃO Nº 363/2021. Conselho Nacional de Justiça. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3668>. Acesso em: 31 mar. 2021

RODOTÁ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RESOLUÇÃO Nº 332/20. Conselho Nacional da Justiça. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 20 mar, 2021.

SANDEL, M. *Contra a perfeição*. Rio de Janeiro, Civilização Brasileira, 2013.

SCHWAB, Klaus. *A quarta revolução industrial*. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016

SCHWABE, J. *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. MARTINS, Leonardo; HENNIG, Beatriz et al (trad). Uruguai: Konrad-Adenauer Stiftung – KAS 2005.

SOLOVE, Daniel. *The Digital Person: Technology and Privacy in the Information Age*. New York University Press: New York, 2004.

WARREN, Samuel D; BRANDEIS, Louis D. *The Right to Privacy*. Harvard Law Review, Vol. 4, N. 5, p.193-220, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 22 mar, 2020.

WASHINGTON, Anne L. How To argue with na algorithm: lessons from the COMPAS-Propublica debate. *The Colorado Technology Law Journal*. v. 17, p. 1-37, 2019. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3357874](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3357874). Acesso em: 09 abr. 2021

---

# **A Proteção da Privacidade dos Denunciantes à luz da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro, relativa à Proteção das Pessoas que denunciem violações do Direito da União**

*Joana Capaz Coelho<sup>117</sup>*

## **RESUMO**

A Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro, relativa à proteção das pessoas que denunciem violações do direito da União, que visa a criação de um conjunto de normas mínimas comuns aos diversos Estados-Membros que protejam, eficazmente, aqueles que, no contexto profissional (seja este público ou privado), tendo obtido conhecimento de ameaças ou situações lesivas do interesse público, as denunciem, terá de ser transposta para os ordenamentos jurídicos dos Estados-Membros até ao dia 17 de dezembro de 2021.

A 29 de abril de 2021, foi aprovada, pelo Conselho de Ministros português, a Proposta de Lei n.º 91/XIV, que visa transpor para o ordenamento jurídico nacional a mencionada Diretiva, a qual veio a ser aprovada, com ligeiras alterações pela Assembleia da República no dia 26 de novembro de 2021.

Os denunciantes assumem um papel central na descoberta e investigação das infrações cometidas no contexto profissional, sendo por isso essencial garantir a confidencialidade da identidade daqueles, de forma a proteger os denunciantes contra qualquer ato de retaliação.

Assim, propomo-nos a analisar de que forma a Diretiva (UE) 2019/1937 garante a proteção de dados e a confidencialidade das informações obtidas num contexto onde se pretende que haja mais transparência e um sério combate à fraude e à corrupção, tanto no Estado como nas Empresas.

## **PALAVRAS-CHAVE**

Denunciante, Confidencialidade, Fraude, Diretiva (UE) 2019/1937, Proposta de Lei n.º 91/XIV.

---

<sup>117</sup> Mestre em Direito, com especialização em Direito Público, pela Faculdade de Direito da Universidade Nova de Lisboa (FDUNL), pós-graduada em Direitos Humanos pelo *Ius Gentium Conimbrigae*/ Centro de Direitos Humanos (IGC/CDH) da Faculdade de Direito da Universidade de Coimbra (FDUC), pós - graduada em Concessões e Parcerias Público-Privadas pelo Instituto de Ciências Jurídico-Políticas (IGJP) da Faculdade de Direito da Universidade de Lisboa (FDUL) e licenciada em Direito pela Faculdade de Direito da Universidade Católica Portuguesa (Escola de Lisboa).

---

# The Protection of Privacy of Whistleblowers under Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the Protection of persons who report breaches of Union Law

*Joana Capaz Coelho*

## ABSTRACT

Directive (UE) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which aims to establish a set of minimum standards common to the various Member States to provide effective protection for those who, in the course of their work (whether public or private), become aware of threats or situations affecting the public interest and report them, will have to be transposed into the Member States' legal systems by 17 December 2021.

On April 29, 2021, the Portuguese Council of Ministers approved the Proposed Law n° 91/XIV/2, which aims to transpose the mentioned Directive into national law, was approved, with minor changes, by the Portuguese Parliament on 26 November 2021.

Whistleblowers play a central role in uncovering and investigating breaches committed in the professional context, and it is therefore essential to guarantee the confidentiality of their identity in order to protect whistleblowers against any act of retaliation.

Thus, we propose to analyze how Directive (EU) 2019/1937 guarantees data protection and the confidentiality of information obtained in a context where more transparency and a serious fight against fraud and corruption are sought, both in the State and in Companies.

## KEYWORDS

Whistleblowers, Confidentiality, Fraud, Directive (EU) 2019/1937, the Proposed Law n° 91/XIV/2.

## Introdução

A corrupção e a fraude constituem, numa economia globalizada, um fenómeno de carácter transnacional e multidimensional com dimensões políticas, económicas, sociais e culturais, que mina as sociedades e as economias, enfraquece os Estados e as democracias e ameaça a sua estabilidade e segurança, na medida em que compromete o desenvolvimento económico e, conseqüentemente, a justiça e a paz social.

Pela relevância que assumem no plano internacional e pelo impacto que projetam, várias têm sido as instâncias que se têm focado no desenvolvimento da prevenção e na luta contra a corrupção, nomeadamente, a Organização das Nações Unidas através da aprovação da Convenção das Nações Unidas contra a Corrupção, a 31 de outubro de 2003.

No Espaço Europeu é hoje evidente que só uma colaboração estruturada entre instituições, órgãos, organismos e agências da União Europeia e dos Estados-Membros e uma cooperação estreita e permanente entre as diferentes autoridades nacionais permitirá um combate eficaz à corrupção.

Porém, se por um lado há que combater a corrupção com firmeza, por outro lado, e com igual determinação, há que proteger os direitos fundamentais, os dados pessoais, daqueles que denunciam as situações de fraude.

Nessa medida, a União Europeia e os Estados-Membros têm vindo a construir um edifício jurídico com a mesma robustez do existente para o combate à fraude e à corrupção, no qual assumem especial relevância a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União, e que visa a criação de um conjunto de normas mínimas comuns aos diversos Estados-Membros que protejam, eficazmente, aqueles que, no contexto profissional (seja este público ou privado), tendo obtido conhecimento de ameaças ou situações lesivas do interesse público, as denunciem.

Nesta ambiência, uma reflexão sobre o tema: "A proteção da Privacidade dos denunciantes e a Diretiva (UE), 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro, relativa à proteção das pessoas que denunciem violações do direito da União" assume especial relevância, atento o papel central dos denunciantes na descoberta e investigação das infrações cometidas no contexto profissional, na importância de garantir a confidencialidade e segurança das informações obtidas e, desta forma, proteger os denunciantes contra qualquer ato de retaliação.

Julgamos, assim, tratar-se de um tema não só atual como pertinente, tendo em conta que a mencionada Diretiva terá de ser transporta para os ordenamentos jurídicos dos Estados-Membros até ao dia 17 de dezembro de 2021.

No caso nacional, a Proposta de Lei n.º 91/XIV, que operará a transposição da Diretiva (UE) 2019/1937 para o ordenamento jurídico nacional, foi aprovada pela Assembleia da República no dia 26 de novembro de 2021, e vai ao encontro da Estratégia Nacional Anticorrupção 2020-2024 aprovada pela Resolução do Conselho de Ministros n.º 37/2021, de 4 de junho de 2021<sup>118</sup>.

---

<sup>118</sup> Resolução do Conselho de Ministros n.º 37/2021, de 4 de junho de 2021, Disponível em <https://dre.pt/home/-/dre/160893669/details/maximized> (consultado a 17.10.2021).



A artigo encontra-se dividido em três Partes: (i) Parte I incide sobre o enquadramento legal do direito à privacidade do denunciante nos planos internacional, europeu e nacional; (ii) Parte II, a partir da análise da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, examinamos em que medida é garantida a proteção dos dados pessoais e a confidencialidade da identidade dos denunciante à luz do direito europeu; (iii) Parte III trata, brevemente, sobre a Proposta de Lei n.º 91/XIV. Iremos concluir com a apresentação dos pontos-chave tratados ao longo do artigo.

## 1. Do Direito à Privacidade do Denunciante

### 1.1. Do direito à Privacidade do Denunciante nos Direitos Internacional e Europeu

Decorre do artigo 12.º da Declaração Universal dos Direitos Humanos (doravante DUDH)<sup>119</sup> que: “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei”.

Com a aprovação da suprarreferida disposição, a Organização das Nações Unidas (abreviadamente ONU), em 10 de dezembro de 1948, ponderou adotar um instrumento internacional relativo à proteção de dados, mas só com a Convenção 108 do Conselho da Europa, aberta à assinatura em 21 de janeiro de 1981, foi adotado o primeiro diploma internacional juridicamente vinculativo neste domínio (“Soft Law”), o qual visa garantir a todas as pessoas singulares o respeito pelos seus direitos e liberdades fundamentais, e, especialmente, pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal.

Mais tarde, em 1966, com a aprovação do Pacto Internacional sobre os Direitos Cívicos e Políticos (PIDCP)<sup>120</sup>, o direito à reserva da vida privada e familiar ficou salvaguardado no seu artigo 17.º. Neste contexto, o Comité dos Direitos Humanos, que monitoriza a implementação do PIDCP, formulou um Comentário Geral particularmente relevante, o n.º 16º, de 1988, sobre o direito ao respeito da privacidade, família, domicílio e correspondência e proteção da honra e reputação.

No que concerne à proteção dos dados do denunciante, é particularmente relevante a Convenção das Nações Unidas contra a Corrupção<sup>121</sup> adotada pela Assembleia Geral das Nações Unidas em 31 de Outubro de 2003, que no seu artigo 33.º, determina que os Estados Parte deverão considerar a incorporação, nos seus sistemas jurídicos internos, de medidas adequadas a assegurar a proteção contra qualquer tratamento injustificado de quem preste, às autoridades competentes, de boa fé e com base em suspeitas razoáveis, informações sobre quaisquer factos relativos às infrações abrangidas pela referida Convenção.

<sup>119</sup> Declaração Universal dos Direitos Humanos, disponível em <https://dre.pt/declaracao-universal-dos-direitos-humanos> (consultado a 03/10/2021).

<sup>120</sup> Pacto sobre os direitos civis e políticos, disponível em [https://adcc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto\\_internacional\\_sobre\\_os\\_direitos\\_civis\\_e\\_politicos.pdf](https://adcc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto_internacional_sobre_os_direitos_civis_e_politicos.pdf) (consultado a 03/10/2021).

<sup>121</sup> Convenção das Nações Unidas contra a Corrupção, disponível em <https://dre.pt/application/dir/pdf1sdiip/2007/09/18300/0669706738.PDF> (consultado a 03/10/2021).

No plano europeu, o artigo 8.º, n.º 1 da Convenção Europeia dos Direitos do Homem (doravante CEDH)<sup>122</sup>, prevê que: “Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”. Por outro lado, o n.º 2 consagra que “Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico, do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros”.

Ensina NUNO SALDANHA que: “Em 1959, com a criação do Tribunal Europeu dos Direitos do Homem (TEDH), a proteção dos direitos individuais ficou definitivamente consagrada quando o próprio TEDH esclareceu que o artigo 8.º da CEDH obrigava não só os Estados a absterem-se de praticar atos suscetíveis de violarem os direitos aí consagrados, como impôs uma atitude positiva por forma a garantirem o respeito efetivo pela vida familiar e privada”<sup>123</sup>.

Ao nível da União Europeia, a nossa atenção deve centrar-se no artigo 16.º, n.º 1 do Tratado de Funcionamento da União Europeia (TFUE)<sup>124</sup> e na Carta de Direitos Fundamentais da União Europeia (CDFUE)<sup>125</sup>, artigos 7.º e 8.º. Nos referidos artigos podemos denotar a preocupação dos Estados em reconhecer tanto o direito ao respeito pela vida privada e familiar, assim como a proteção de dados pessoais, o que está em consonância com o artigo 39.º do Tratado da União Europeia (TUE)<sup>126</sup>.

Neste domínio, 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 de Proteção de Dados-RGPD)<sup>127</sup> — que revoga a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados<sup>128</sup> — tem vindo a adquirir uma crescente relevância, estabelecendo a proteção das pessoas singulares relativamente ao tratamento de dados pessoais como um direito fundamental, tendo sido aprovado em 27 de abril de 2016 e tendo aplicação obrigatória no Ordenamento Jurídico português e no dos restantes países que integram a UE desde 25 de maio de 2018.

---

<sup>122</sup>Convenção Europeia dos Direitos do Homem, disponível em [https://www.echr.coe.int/documents/convention\\_por.pdf](https://www.echr.coe.int/documents/convention_por.pdf) (consultado a 03/10/2021).

<sup>123</sup>In “RGPD - GUIA PARA UMA AUDITORIA DE CONFORMIDADE, DADOS, PRIVACIDADE, IMPLEMENTAÇÃO, CONTROLO E COMPLIANCE”, FCA – Editora de Informática, Lda, 2019, p.11.

<sup>124</sup>Tratado de Funcionamento da União Europeia, disponível em [https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC\\_3&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF) (consultado a 03/10/2021).

<sup>125</sup>Carta de Direitos Fundamentais da União Europeia, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR> (consultado a 03/10/2021).

<sup>126</sup> Tratado da União Europeia, disponível em [https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF) (consultado a 03/10/2021).

<sup>127</sup> Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Proteção de Dados-RGPD), disponível em disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679> (consultado a 03/10/2021).

<sup>128</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046> (consultado a 03/10/2021).

No que concerne à proteção dos dados dos denunciantes, há que ter em conta a Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União, que, como veremos, designadamente nos seus artigos 16.º, 17.º e 18.º, garante a confidencialidade da identidade daqueles que tendo obtido conhecimento de situações lesivas do interesse público, as denunciem.

## 1.2. Do direito à Privacidade no Direito Nacional

O artigo 26.º da Constituição da República Portuguesa (CRP)<sup>129</sup>, consagra o direito à reserva e intimidade da vida privada, o qual haverá de ser conjugado com o disposto no artigo 16.º da mesma CRP, que estabelece que os direitos fundamentais consagrados na Constituição não excluem quaisquer outros constantes das leis e das regras aplicáveis de direito internacional.

Por seu turno, o artigo 16, n.º 2, da CRP prevê que os preceitos constitucionais e legais relativos aos direitos fundamentais devem ser interpretados e integrados de harmonia com a DUDH.

Da maior importância é o n.º 1 do artigo 35.º da CRP, nos termos do qual: “Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei”.

Em 1991, entrou em vigor a Lei n.º 10/91, de 9 de abril (Lei da Proteção de Dados Pessoais face à informática) e com ela foi criada a Comissão Nacional de Proteção de Dados Pessoais Informatizados (CNPDPPI).

A CNPDPPI passou a designar-se Comissão Nacional de Proteção de Dados (CNPD) com a entrada em vigor da Lei n.º 67/98, de 26 de outubro (Lei que transpôs para o Ordenamento Jurídico Nacional a Diretiva 95/46/CE).

Em 2019, entrou em vigor a Lei n.º 58/2019 — Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Em relação à proteção dos dados do denunciante, ainda não foi transposta para o ordenamento jurídico nacional a Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União, e que terá de ser transposta para os diversos ordenamentos jurídicos dos Estados-Membros.

Na presente data, a principal Lei que protege os denunciantes contra potenciais atos de retaliação é a Lei 19/2008, que aprova medidas de combate à corrupção e procede à primeira alteração à Lei n.º 5/2002, de 11 de janeiro, à décima sétima alteração à lei geral tributária e à terceira alteração à Lei n.º 4/83, de 2 de abril<sup>130</sup>.

<sup>129</sup> Constituição da República Portuguesa, disponível em <https://dre.pt/legislacao-consolidada/-/lc/34520775/view> (consultado a 03/10/2021).

<sup>130</sup> Lei 19/2008 - aprova medidas de combate à corrupção e procede à primeira alteração à Lei n.º 5/2002, de 11 de janeiro, à décima sétima alteração à lei geral tributária e à terceira alteração à Lei n.º 4/83, de 2 de abril, disponível em <https://dre.pt/pesquisa/-/search/249976/details/maximized> (consultado 05.10.2021).

## **2. Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019**

### **2.1. Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Aspectos Gerais**

A Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019<sup>131</sup>, relativa à proteção das pessoas que denunciem violações do direito da União, que entrou em vigor no dia 17 de dezembro de 2019, terá de ser transposta para os ordenamentos jurídicos dos Estados-Membros até ao dia 17 de dezembro de 2021 (2 anos contados da data da entrada em vigor daquela Diretiva).

A Diretiva (UE) 2019/1937 tem como objetivo a criação de um conjunto de normas mínimas comuns aos diversos Estados-Membros que protejam, eficazmente, os denunciadores<sup>132</sup> (whistleblowers), que, no contexto profissional (seja este público ou privado), tendo obtido conhecimento de ameaças ou situações lesivas do interesse público, as denunciem.

Para NUNO BRANDÃO, Whistleblowing pode ser definido como: “a atividade daquele que sinaliza um comportamento ilegal ou irregular ocorrido no quadro de uma organização, pública ou privada, com a qual tem ou teve algum vínculo”<sup>133</sup>.

Decorre, aliás, do Considerando primeiro da Diretiva (UE) 2019/1937 que: “As pessoas que trabalham numa organização pública ou privada ou que com ela estão em contato no contexto de atividades profissionais são frequentemente as primeiras a ter conhecimento de ameaças ou de situações lesivas do interesse público que surgem nesse contexto. Ao denunciar violações do direito da União lesivas do interesse público, essas pessoas agem como denunciadores, desempenhando assim um papel essencial na descoberta e prevenção dessas violações, bem como na salvaguarda do bem-estar na sociedade. Todavia, os potenciais denunciadores são frequentemente desencorajados de comunicar as suas preocupações ou suspeitas por receio de retaliação. Neste contexto, a importância de assegurar um nível equilibrado e eficaz de proteção dos denunciadores é cada vez mais reconhecida, tanto ao nível da União como ao nível internacional”.

Os denunciadores assumem um papel central na descoberta, investigação e prevenção das infrações cometidas no contexto profissional e, nesta medida, a sua privacidade deve ser protegida com determinação, de modo a criar-se um ambiente seguro que permita a denuncia das infrações cometidas dentro das organizações jurídicas<sup>134</sup>.

Neste âmbito, a Diretiva (UE) 2019/1937 pretende, como veremos, por um lado, proteger aqueles que, de boa-fé, denunciem infrações cometidas no contexto laboral

---

<sup>131</sup> Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L1937&from=en> (consultado a 17.10.2021).

<sup>132</sup> Já de acordo com o artigo 5.º da Proposta de Lei n.º 91/XIV: “*Considera-se denunciante qualquer pessoa singular que denuncie ou divulgue publicamente uma infração com fundamento em informações obtidas no âmbito da sua atividade profissional, quer esta seja exercida no setor público quer no setor privado e independentemente da sua natureza*”.

<sup>133</sup> “O Whistleblowing no ordenamento jurídico português”, Nuno Brandão, Revista do Ministério Público 161: janeiro-março 2020, pp.99-113, p.99.

<sup>134</sup> Da exposição de motivos da Proposta de Lei n.º 91/XIV pode ler-se que: “*As pessoas que trabalham numa organização pública ou privada, ou que com elas contactam profissionalmente, estão, por vezes, numa posição privilegiada para tomar conhecimento de ameaças ou de lesões efetivas que surgem no contexto dessas organizações, mas estão igualmente expostas a retaliações, com incidência na sua situação laboral, o que constitui um importante fator de inibição e de injustiça*”.

de posteriores atos de retaliação e, por outro lado, prevenir a prática destas infrações dentro das organizações.

## **2.2. Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Âmbito de Aplicação**

O artigo 4.º da Diretiva (UE) 2019/1937 incide sobre o âmbito de aplicação subjetivo do diploma.

De acordo com o supramencionado artigo, a Diretiva (UE) 2019/1937 abrange os denunciantes que exercem funções (no setor público ou privado) e que tenham obtido informações sobre ameaças ou situações lesivas do interesse público.

Deste modo, são denunciantes para efeitos da Diretiva (UE) 2019/1937, nomeadamente:

- Os trabalhadores, na aceção do artigo 45.º, n.º 1, do TFUE, incluindo trabalhadores públicos (cfr. n.º 1, al. a) do artigo 4.º da Diretiva);
- Não assalariados, na aceção do artigo 49.º do TFUE (cfr. n.º 1, al. b) do artigo 4.º da Diretiva);
- Titulares de participações sociais e pessoas pertencentes a órgãos de administração, de gestão ou de supervisão de empresas, incluindo membros não executivos, assim como voluntários e estagiários remunerados ou não remunerados (cfr. n.º 1, al. c) do artigo 4.º da Diretiva) e, ainda;
- Quaisquer pessoas que trabalhem sob a supervisão e a direção de contratantes, subcontratantes e fornecedores (cfr. n.º 1, al. d) do artigo 4.º da Diretiva).

A Diretiva (UE) 2019/1937 cobre, também, os denunciantes que comuniquem informações sobre violações obtidas numa relação profissional que já tenha terminado (n.º 2 do artigo 4.º) e os denunciantes cuja relação profissional ainda não se tenha iniciado, nos casos em que se tenha cometido violações durante o processo de recrutamento ou noutra fase de negociação pré-contratual (n.º 3 do artigo 4.º).

Significa isto que a Diretiva (UE) 2019/1937 se aplica a sujeitos que obtenham conhecimento de violações praticadas dentro do seu seio profissional e não a pessoas estranhas a esse contexto profissional, salvo exceções<sup>135</sup>.

Relativamente ao âmbito de aplicação material da Diretiva (UE) 2019/1937, decorre do artigo 2.º que<sup>136</sup> as violações abrangidas pela Diretiva dizem respeito aos seguintes domínios:

- Contratação Pública (vide n.º 1, al. i) do artigo 2.º da Diretiva (UE) 2019/1937);

---

<sup>135</sup> Decorre do n.º 4 do artigo 4.º da Diretiva que: "As medidas de proteção de denunciantes estabelecidas no capítulo IV são igualmente aplicáveis, se for caso disso a: a) Facilitadores; b) Terceiros que estejam ligados aos denunciantes e que possam ser alvo de retaliação num contexto profissional, tais como colegas ou familiares dos denunciantes; e) Entidades jurídicas que sejam detidas, para as quais os denunciantes trabalhem ou com as quais estejam de alguma forma ligados num contexto profissional".

<sup>136</sup> Determina o Considerando 19 da Diretiva que: "O artigo 2.º, n.º 1, alínea a), define o âmbito de aplicação material da presente diretiva através de uma remissão para uma lista de atos da União constante do anexo. Tal implica que, sempre que esses atos da União, por sua vez, definam o respetivo âmbito de aplicação material por remissão para atos da União enumerados nos respetivos anexos, estes últimos atos fazem também parte do âmbito de aplicação material da presente diretiva. Além disso, a remissão para os atos no anexo deverá ser entendida como incluindo todas as medidas delegadas ou de execução, nacionais e da União, adotadas nos termos desses atos. Acresce que a remissão para atos da União no anexo deverá ser entendida como uma remissão dinâmica, de acordo com o sistema padrão de referência dos atos jurídicos da União. Assim, caso um ato da União no anexo tenha sido ou seja alterado, a remissão diz respeito ao ato tal como alterado; caso um ato da União no anexo tenha sido ou seja substituído, a remissão diz respeito ao novo ato".

- Serviços, produtos e mercados financeiros e prevenção do branqueamento de capital e do financiamento ao terrorismo (vide n.º 1, al. ii) do artigo 2.º da Diretiva (UE) 2019/1937);
- Segurança e conformidade dos produtos (vide n.º 1, al. iii) do artigo 2.º da Diretiva (UE) 2019/1937);
- Segurança dos transportes (vide n.º 1, al. iv) do artigo 2.º da Diretiva (UE) 2019/1937);
- Proteção do ambiente (vide n.º 1, al. v) do artigo 2.º da Diretiva (UE) 2019/1937);
- Proteção contra radiações e segurança nuclear (vide n.º 1, al. vi) do artigo 2.º da Diretiva (UE) 2019/1937);
- Segurança dos géneros alimentícios e dos alimentos para animais, saúde e bem-estar animal nuclear (vide n.º 1, al. vii) do artigo 2.º da Diretiva (UE) 2019/1937);
- Saúde pública (vide n.º 1, al. viii) do artigo 2.º da Diretiva (UE) 2019/1937);
- Defesa do consumidor (vide n.º 1, al. ix) do artigo 2.º da Diretiva (UE) 2019/1937);
- Proteção da privacidade e dos dados pessoais e segurança da rede e dos sistemas de informação (vide n.º 1, al. x) do artigo 2.º da Diretiva (UE) 2019/1937).

### **2.3. Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Canais de Denúncia e Respetivos Procedimentos**

De acordo com a Diretiva (UE) 2019/1937, as entidades jurídicas dos setores privados e público serão obrigadas a implementar canais e procedimentos de denúncia interna (artigos 7.º a 9.º) e externa (artigos 10.º a 14.º).

Estes canais de denúncia devem garantir a privacidade, confidencialidade e segurança das denúncias<sup>137</sup>. Como explica PATRICK DE PITTA SIMÕES: *“Todavia, os denunciadores são frequentemente desencorajados de comunicar as suas preocupações ou suspeitas por receio de retaliação. Daí que, seja necessário protegê-los através de canais confidenciais e seguros, que assegurem uma proteção eficaz contra atos de descrédito ou represálias”*<sup>138</sup>.

Decorre do Considerando 60 da Diretiva (UE) 2019/1937 que: *“a deteção e a prevenção eficazes de violações do direito da União requerem a garantia de que os potenciais denunciadores possam comunicar, facilmente e com total confidencialidade, as informações de que dispõem às autoridades competentes para investigar e solucionar o problema, sempre que possível”* (sublinhado nosso).

<sup>137</sup> Determina o Considerando 74 da Diretiva (UE) 2019/1937 que: *“O pessoal das autoridades competentes que é responsável pelo tratamento das denúncias, deverá ter formação profissional, nomeadamente sobre as normas aplicáveis em matéria de proteção de dados, para tratar das denúncias e assegurar a comunicação com os respetivos denunciadores, bem como para dar o seguimento adequado à denúncia”* e do Considerando (77): *“ É necessário que o pessoal da autoridade competente, que é responsável pelo tratamento de denúncias, e o pessoal da autoridade competente, que tem direito a aceder às informações prestadas pelo denunciante, respeitem o dever de segredo profissional e de confidencialidade na transmissão dos dados no interior e para o exterior da autoridade competente, nomeadamente quando esta inicia uma investigação ou abre um inquérito interno, ou participa em atividades de aplicação da lei relacionadas com a denúncia”*.

<sup>138</sup> In “O Whistleblowing é um assunto de Polícia (s)?”, Cedis Working Papers, setembro 2020, p.15.



E do Considerando 73 da supramencionada Diretiva: “A fim de permitir uma comunicação eficaz com o pessoal responsável por tratar das denúncias, as autoridades competentes deverão criar canais que sejam fáceis de utilizar, seguros, garantam a confidencialidade para receber e tratar as informações prestadas pelo denunciante sobre violações e permitam o armazenamento duradouro de informações para permitir investigações mais aprofundadas (...)” (sublinhado nosso).

Como veremos, é fundamental proteger os denunciantes, desde logo contra potenciais atos de retaliação, sendo, por isso, essencial garantir que estes canais de denúncia protejam os direitos fundamentais dos denunciantes, desde logo, o direito à proteção dos dados pessoais.

Neste sentido, “os Estados-Membros deverão assegurar que as autoridades competentes disponham de procedimentos de proteção adequados para tratar as denúncias e para proteger os dados pessoais das pessoas nelas referidas. Esses procedimentos deverão garantir que as identidades de todos os denunciantes, das pessoas visadas e de terceiros referidos na denúncia, por exemplo, testemunhas ou colegas estejam protegidas em todas as fases do procedimento” (sublinhado nosso). (cfr. Considerando 76 da Diretiva).

### **2.3.1 Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Canais de Denúncia Interno e respetivos Procedimentos**

Determina o n.º 2 do artigo 7.º da Diretiva (UE) 2019/1937 que os Estados-Membros deverão incentivar a denúncia através dos canais internos de denúncia, sempre que a violação possa ser eficazmente resolvida a nível interno e sempre que o denunciante considere não existir risco de retaliação.

Decorre do artigo 8.º, n.º 1, da Diretiva (UE) 2019/1937, que os Estados-Membros (EM) devem assegurar que as entidades jurídicas do sector privado e público estabeleçam canais e procedimentos para denúncia interna e para o seguimento, após consultas e em acordo com os parceiros sociais, sempre que previsto no direito nacional.

O supramencionado artigo aplica-se, designadamente, a entidades jurídicas do setor privado com 50 ou mais trabalhadores (cfr. n.º 3 do artigo 8.º da Diretiva (UE) 2019/1937), com exceção das entidades abrangidas pelo âmbito de aplicação dos atos da União a que se referem a parte I.B e a parte II do anexo.

Já no caso das entidades jurídicas do setor público, os Estados-Membros podem dispensar da obrigação a que se refere o n.º 1 os municípios com menos de 10 000 habitantes ou menos de 50 trabalhadores (cfr. n.º 9 do artigo 8.º da Diretiva (UE) 2019/1937).

Relativamente aos procedimentos para denúncias internas e seguimento, prevê o artigo 8.º da Diretiva (UE) 2019/1937 que neste conceito se incluem:

– Canais para receção de denúncias que sejam concebidos, instalados e operados de forma segura, de forma a garantir que a confidencialidade da identidade

dos denunciantes e dos terceiros mencionados na denúncia seja protegida e a impedir o acesso de pessoal não autorizado (cfr. al. a) do n.º 1 do artigo 9.º da Diretiva)<sup>139</sup>;

– Avisos de receção da denúncia ao denunciante num prazo de sete dias a contar da data da receção (cfr. al. b) do n.º 1 do artigo 9.º da Diretiva);

– A designação de uma pessoa ou serviço imparcial competente para dar seguimento às denúncias, que pode ser a mesma pessoa ou o mesmo departamento que recebe e que manterá a comunicação com o denunciante e, se necessário, que solicitará mais informações e dará ao denunciante retorno de informação (cfr. al. c) do n.º 1 do artigo 9.º da Diretiva);

– O seguimento diligente pela pessoa ou serviço designado a que se refere a alínea c) (cfr. al. d) do n.º 1 do artigo 9.º da Diretiva);

– O seguimento diligente, sempre que previsto no direito nacional, de denúncias anónimas (cfr. al. e) do n.º 1 do artigo 9.º da Diretiva);

– Um prazo razoável para dar retorno de informação, que não exceda três meses a contar do aviso de receção ou, se este não tiver sido enviado ao denunciante, três meses a contar do termo do prazo de sete dias após a apresentação da denúncia (cfr. al. f) do n.º 1 do artigo 9.º da Diretiva) e, finalmente,

– A prestação de informações claras e facilmente acessíveis sobre os procedimentos para efetuar denúncias externas às autoridades competentes, nos termos do artigo 10.º, e, se aplicável, às instalações, órgãos ou organismos da União (cfr. al. g) do n.º 1 do artigo 9.º da Diretiva).

Decorre do artigo 9.º, n.º 2, da Diretiva (UE) 2019/1937 que os canais de denúncia devem possibilitar a apresentação de denúncias, verbalmente ou por escrito. A denúncia verbal deve ser possível de realizar por telefone, através de outros sistemas de mensagens de voz ou através de reunião presencial, caso tal seja solicitado pelo denunciante.

---

<sup>139</sup> Determina o Considerando 3 da Diretiva (UE) 2019/1937 que: "(...) sempre que se detetem deficiências na aplicação do direito nesses domínios, e os denunciantes encontram-se geralmente em posição privilegiada para as divulgar, será necessário reforçar a aplicação do direito, estabelecendo canais de denúncia eficazes, confidenciais e seguros e assegurando uma proteção eficaz dos denunciantes contra atos de retaliação".



### 2.3.2 Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Canais de Denúncia Externa e respectivos Procedimentos

Resulta do artigo 10.º da Diretiva (UE) 2019/1937 que os canais de denúncia externa devem ser utilizados após os denunciante terem apresentado uma denúncia através dos canais de denúncia interna, podendo, ainda assim, ser apresentadas denúncias diretamente através de canais de denúncia externa. Significa isto que o denunciante pode optar pela via que preferir.

Os Estados-Membros devem designar trabalhadores competentes para receber, dar retorno de informação e dar seguimento às denúncias, e devem dotá-las dos recursos físicos/tecnológicos adequados.

Nesta ambiência, os EM devem assegurar que as autoridades competentes:

— Estabelecem canais de denúncia externa independentes e autónomos, para receber e tratar as informações sobre violações (vide, al. a) do n.º 2 do artigo 11.º);

— Acusem a receção da denúncia prontamente e, em qualquer caso, no prazo de sete dias a contar da sua receção, salvo pedido expresso em contrário do denunciante ou se a autoridade competente tiver motivos razoáveis para crer que o aviso de receção da denúncia comprometeria a proteção da identidade do denunciante (vide, al. b) do n.º 2 do artigo 11.º);

— Deem um seguimento diligente às denúncias do denunciante (vide, al. c) do n.º 2 do artigo 11.º);

— Deem ao denunciante retorno de informação sobre o seguimento dado à denúncia num prazo razoável não superior a três meses, ou a seis meses em casos devidamente justificados (vide, al. d) do n.º 2 do artigo 11.º);

— Comuniquem ao denunciante o resultado final das investigações desencadeadas pela denúncia, em conformidade com procedimentos previstos no direito nacional (vide, al. e) do n.º 2 do artigo 11.º);

— Transmitam em tempo útil as informações contidas na denúncia às instituições, órgãos ou organismos da União competentes, conforme for adequado, para investigação mais aprofundada, sempre que tal esteja previsto no direito da União ou no direito nacional (vide, al. f) do n.º 2 do artigo 11.º).

Para efeitos do artigo 12.º da Diretiva (UE) 2019/1937, são considerados independentes e autónomos os canais de denúncia externa que satisfaçam cumulativamente os seguintes critérios<sup>140</sup>:

- a) Serem concebidos, instalados e operados de forma a assegurar a exaustividade, a integridade e a confidencialidade das informações e a impedir o acesso de pessoal não autorizado da autoridade competente (**negrito nosso**);
- b) Possibilitarem o armazenamento de informações duradouras, nos termos do artigo 18.º, para permitir a realização de investigações mais aprofundadas.

---

<sup>140</sup> Artigo 12.º, n.º3 da Diretiva (UE) 2019/1937 dispõe que: "As autoridades competentes asseguram que, sempre que as denúncias forem recebidas por canais que não sejam os canais para denúncia a que se referem os n.ºs 1 e 2 ou por pessoal que não seja o responsável pelo tratamento das denúncias, é proibido ao pessoal que as tiver recebido divulgar informações que possam identificar o denunciante ou a pessoa visada e que as informações são imediatamente transmitidas, sem qualquer modificação, ao pessoal responsável pelo tratamento de denúncias".

Os Estados Membros devem ainda assegurar que as autoridades competentes publiquem, em secção separada, facilmente identificável e acessível dos respetivos sítios Web, pelo menos, as seguintes informações:

— As condições para os denunciantes beneficiarem de proteção ao abrigo da presente Diretiva (*cfr.* al. a) do artigo 13.º);

— Os dados de contacto dos canais de denúncia externa, como previsto no artigo 12.º, em especial os endereços eletrónicos e postais, e os números de telefone dos referidos canais, com indicação sobre se as comunicações telefónicas são gravadas (*cfr.* al. b) do artigo 13.º);

— Procedimentos aplicáveis à denúncia de violações, nomeadamente a forma pela qual a autoridade competente pode solicitar ao denunciante que clarifique as informações comunicadas ou que preste informações adicionais, o prazo para dar retorno de informação e o tipo e conteúdo desse retorno de informação (*cfr.* al. c) do artigo 13.º);

— O regime de confidencialidade aplicável às denúncias, em particular informações sobre o tratamento de dados pessoais, nos termos do artigo 17.º da presente diretiva, os artigos 5.º e 13.º do Regulamento (UE) 2016/679, o artigo 13.º da Diretiva (UE) 2016/680 e o artigo 15.º do Regulamento (UE) 2018/1725, consoante o caso (*cfr.* al. d) do artigo 13.º) (**negrito nosso**);

— Natureza do seguimento a dar às denúncias (*cfr.* al. e) do artigo 13.º);

— Vias de recurso e procedimentos de proteção contra atos de retaliação e disponibilidade de aconselhamento confidencial para as pessoas que ponderam efetuar uma denúncia (*cfr.* al. f) do artigo 13.º);

— Declaração em que se explique claramente as condições em que quem efetuar uma denúncia à autoridade competente não incorre em responsabilidade por violação da confidencialidade nos termos do artigo 21.º, n.º 2 (*cfr.* al. g) do artigo 13.º);

— Os contactos do centro de informação ou da autoridade administrativa independente única prevista no artigo 20.º, n.º 3, consoante aplicável (*cfr.* al. h) do artigo 13.º).

### **2.3.3 Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Confidencialidade**

Nos termos do prescrito no artigo 16.º, n.º 1 da Diretiva (UE) 2019/1937: “*Os Estados-Membros asseguram que a identidade do denunciante não seja divulgada a ninguém, para além do pessoal autorizado competente para receber denúncias ou a estas dar seguimento, sem o consentimento explícito do denunciante (...)*”.

O artigo 16.º, n.º 2, prevê as exceções ao n.º 1. Nesta ambiência, a identidade do denunciante apenas pode ser divulgada se tal constituir uma obrigação necessária e proporcionada imposta pelo Direito da União ou pelo Direito nacional no contexto de uma investigação por autoridades nacionais ou de processos judiciais, inclusive com vista a salvaguardar os direitos de defesa da pessoa visada.

Neste caso, os denunciantes devem ser informados antes da divulgação da sua identidade<sup>141</sup>, salvo se tal informação comprometer as investigações ou processos judiciais relacionados. Ao informar os denunciantes, a autoridade competente deve enviar-lhes uma comunicação por escrito explicando os motivos da divulgação dos dados confidenciais em causa (n.º 3 do artigo 16.º da Diretiva (UE) 2019/1937).

Do artigo 18.º da Diretiva (UE) 2019/1937 resulta que as denúncias devem ser conservadas *“apenas durante o período necessário e proporcionado a fim de dar cumprimento aos requisitos impostos pela presente diretiva ou a outros requisitos impostos pelo direito nacional ou da União”*.

Relativamente ao tratamento de dados. Determina o artigo 17.º da Diretiva (UE) 2019/1937 que este deve ser feito em respeito ao RGPD e à Diretiva (UE) 2016/680.<sup>142</sup>

O intercâmbio e a transmissão de informações entre instituições, órgãos ou organismos da União são efetuados de acordo com o Regulamento (UE) 2018/1725.<sup>143</sup>

No caso dos dados pessoais que manifestamente não forem relevantes para o tratamento de uma denúncia específica não devem ser recolhidos ou, se inadvertidamente o tiverem sido, devem ser apagados sem demora indevida.

### **2.3.4 Da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019: Proibição de Retaliação**

De acordo com o artigo 19.º da Diretiva (UE) 2019/1937, os EM deverão tomar as medidas necessárias para proibir qualquer forma de retaliação (incluindo ameaças de retaliação e tentativas de retaliação), de onde se incluem:

- Suspensão, despedimento ou medidas equivalentes (*cf.* al. a) do artigo 19.º da Diretiva (UE) 2019/1937);
- Despromoção ou não promoção (*cf.* al. b) do artigo 19.º da Diretiva (UE) 2019/1937);
- Alteração de funções, alteração do local de trabalho, redução de salários e alteração do horário de trabalho (*cf.* al. c) do artigo 19.º da Diretiva (UE) 2019/1937);
- Recusa de formação (*cf.* al. d) do artigo 19.º da Diretiva (UE) 2019/1937);

---

<sup>141</sup> Resulta da al. d) do n.º 1 do artigo 23.º da Diretiva (UE) 2019/1937: *“Violam o dever de manutenção da confidencialidade da identidade dos denunciantes, tal como referido no artigo 16.º”*.

<sup>142</sup> Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680> (consultado a 05.10.2021).

<sup>143</sup> Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725> (consulto em 05.10.2021).

- Avaliação negativa do desempenho ou referência negativa para fins de emprego (*cfr.* al. d) do artigo 19.º da Diretiva (UE) 2019/1937);
- Imposição ou administração de qualquer medida disciplinar, admoestação ou outra sanção, inclusivamente financeira (*cfr.* al. f) do artigo 19.º da Diretiva (UE) 2019/1937);
- Coação, intimidação, assédio ou ostracização (*cfr.* al. g) do artigo 19.º da Diretiva (UE) 2019/1937);
- Discriminação, desfavorecimento ou tratamento injusto (*cfr.* al. h) do artigo 19.º da Diretiva (UE) 2019/1937);
- Não conversão de um contrato de trabalho temporário num contrato permanente, sempre que o trabalhador tivesse expectativas legítimas de que lhe seria oferecido emprego permanente (*cfr.* al. i) do artigo 19.º da Diretiva (UE) 2019/1937);
- Não renovação ou rescisão antecipada de um contrato de trabalho temporário (*cfr.* al. i) do artigo 19.º da Diretiva (UE) 2019/1937);
- Danos, inclusivamente à sua reputação, nomeadamente nas redes sociais, ou perda financeira, incluindo perda de negócios e perda de rendimentos (*cfr.* al. j) do artigo 19.º da Diretiva (UE) 2019/1937);
- Inclusão numa lista negra, com base num acordo formal ou informal à escala setorial, que possa implicar a impossibilidade de, no futuro, os denunciantes encontrarem emprego no setor ou na indústria (*cfr.* al. l) do artigo 19.º da Diretiva (UE) 2019/1937);
- Rescisão antecipada ou resolução do contrato de fornecimento de bens ou de prestação de serviços (*cfr.* al. m) do artigo 19.º da Diretiva (UE) 2019/1937);
- Revogação de uma licença ou autorização (*cfr.* al. n) do artigo 19.º da Diretiva (UE) 2019/1937);
- Encaminhamento para tratamento psiquiátrico médico (*cfr.* al. o) do artigo 19.º da Diretiva (UE) 2019/1937).

A proteção dos denunciantes contra atos de retaliação é fundamental para encorajar mais pessoas a denunciar as violações ao direito da União Europeia que ocorrem dentro das organizações jurídicas de direito público e privado. Como já vimos, os denunciantes desempenham um papel fundamental no que concerne à descoberta, investigação e prevenção de ameaças ou situações lesivas do interesse público.

Aliás, decorre do artigo 33.º da Convenção das Nações Unidas contra a Corrupção que: *“cada Estado Parte deverá considerar a incorporação no seu sistema jurídico interno de medidas adequadas para assegurar a proteção contra qualquer tratamento injustificado de quem preste, às autoridades competentes, de boa-fé e com*

base em suspeitas razoáveis, informações sobre quaisquer factos relativos às infrações estabelecidas em conformidade com a presente Convenção”.

Assim, e para além das medidas supra explicadas, a Diretiva (UE) 2019/1937 prevê medidas de apoio aos denunciadores (vide artigo 20.º) e medidas de proteção contra atos de retaliação (vide artigo 21.º).

### **3. Da Transposição para a Ordem Jurídica Interna da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019**

O Conselho de Ministros português aprovou, a 29 de abril de 2021, a Proposta de Lei n.º 91/XIV<sup>144</sup>, doravante por Proposta, que visa a transposição da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União para o ordenamento jurídico nacional.

O Estado português, como, aliás, os restantes EM, terá que transpor a sempre mencionada Diretiva até ao dia 17 de dezembro de 2021.

A Proposta encontra-se alinhada com a Diretiva (UE) 2019/1937 uma vez que “visando dar cumprimento às exigências da União Europeia, prevê a criação de um regime geral de proteção daqueles que, de boa-fé, e com base em informações obtidas em contexto profissional que razoavelmente considerem verdadeiras, denunciem ou divulguem infrações ao direito da União Europeia, conforme previsto na Diretiva, ou atos de criminalidade violenta, especialmente violenta ou altamente organizada”.

Na verdade, e à semelhança do verificado no espaço da União Europeia, também o ordenamento jurídico nacional, apesar da existência de normas de proteção em domínios específicos, não dispõe de um regime transversal de proteção dos denunciadores, o que determina, desde logo, a desnecessidade de previsão de revogações, totais ou parciais, de diplomas legais.

No que concerne, em concreto, à matéria de privacidade e proteção de dados, a Proposta protege, como resulta desde logo dos artigos 9.º, 13.º, 14.º, 16.º<sup>145</sup>,

---

<sup>144</sup> Proposta de Lei n.º 91/XIV, disponível em <https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765247396a6457316c626e527663306c7561574e7059585270646d45764d7a4d7a595451344d546b744d47466a596930304e6a4a6b4c54686c597a55744d6a45325a6d566b4e546b314e545a6b4c6d52765933673d&fich=333a4819-0acb-462d-8ec5-216fed59556d.docx&inline=true> (consultado a 05.10.2021).

<sup>145</sup> Nos termos do artigo 16.º da Proposta de Lei n.º 91/XIV: “As autoridades competentes publicam nos respetivos sítios na Internet, em seção separada, facilmente separada identificável e acessível, pelo menos as seguintes informações:

- d) O regime de confidencialidade aplicável às denúncias, em particular quanto ao tratamento de dados pessoais;
- g) Disponibilidade de aconselhamento confidencial para as pessoas que ponderam apresentar uma denúncia”.

17.º, 24.º<sup>146</sup> e 26.º, o denunciante, tal como acontece com a Diretiva, garantindo a confidencialidade da identidade dos denunciantes.

Quanto aos canais de denúncia interna, determina o n.º 1 do artigo 9.º da mencionada Proposta que estes devem permitir “a apresentação e o seguimento de denúncias, a fim de garantir a confidencialidade da identidade dos denunciantes e de terceiros mencionados na denúncia e impedir o acesso de pessoas não autorizadas” (sublinhado nosso). Ora, tal como se verifica com a Diretiva (UE) 2019/1937, devem ser criados canais de denúncia seguros, que possibilitam a denúncia das infrações cometidas no contexto profissional, sem que com isso se comprometam os direitos fundamentais dos denunciantes, em particular o seu direito fundamental à privacidade – onde se inclui o direito de os denunciantes verem a confidencialidade da sua identidade garantida.

Decorre, ainda, do artigo 9.º, n.º 2 da Proposta, que os canais de denúncia interna são operados internamente, para efeitos de receção e posterior seguimento das denúncias, por pessoas ou serviços designados para o efeito, e do n.º 3 que os canais de denúncia podem ainda ser operados externamente para efeitos de receção de denúncias.

Determina o n.º 4 do artigo 9.º da Proposta que nas situações previstas supra “deve ser garantida a independência, a imparcialidade, a confidencialidade e a proteção de dados, o sigilo e a ausência de conflitos de interesses no desempenho das funções” (sublinhados nosso).

Assim sendo, parece haver um compromisso sério da Proposta na defesa do direito fundamental à privacidade dos denunciantes através da garantia da confidencialidade e da proteção dos dados pessoais dos denunciantes.

É de sublinhar, por outro lado, que constitui contraordenação muito grave, nos termos do disposto no artigo 26, n.º 3, alínea b) da Proposta: “dispor de um canal de denúncia interna sem garantias de confidencialidade da identidade dos denunciantes ou sem regras que impeçam o acesso a pessoas não autorizadas, nos termos do n.º 1 do artigo 9.º” (sublinhado nosso).

Relativamente aos canais de denúncia externa, determina o artigo 13, n.º 1 da Proposta que: “As autoridades competentes estabelecem canais de denúncia externa independentes e autónomos para receber e dar seguimento às denúncias, que assegurem a exaustividade, a integridade e a confidencialidade das informações, impeçam o acesso de pessoas não autorizadas e permitam a conservação de informações nos termos do artigo 19.º” (sublinhados nosso).

---

<sup>146</sup> De acordo com o disposto no artigo 24.º da Proposta de Lei n.º 91/XIV, as pessoas que sejam as autoras da infração ou que a ela estejam associadas estão sujeitas à confidencialidade da identidade do denunciante.

Assim, à luz do disposto no artigo 12.º, alínea a) da Diretiva (UE) 2019/1937, a Proposta consagra canais de denúncia externa que garantam a confidencialidade das informações obtidas e impeçam o acesso de pessoal não autorizado.

Para além disto, estabelece o artigo 26.º, n.º 3, alínea k) da Proposta que constitui contraordenação grave: *“dispor de um canal de denúncia externa que não seja independente e autónomo, ou que não assegure a exaustividade, integridade ou confidencialidade das informações constantes da denúncia, ou que não impeça o acesso a pessoas não autorizadas, nos termos do n.º 1 do artigo 13.º”*.

Resulta, ainda, do artigo 14, n.º 1 da Proposta que os canais de denúncia externa possibilitam a apresentação de denúncias (quer por escrito quer verbalmente) e com a identificação do denunciante ou anonimamente.

Da maior relevância é o que prescreve o artigo 17.º da Proposta, quando determina, no seu n.º 1, que: *“A identidade do denunciante, bem como as informações que, direta ou indiretamente, permitam deduzir a sua identidade, têm natureza confidencial e são de acesso restrito às pessoas responsáveis por receber ou dar seguimento a denúncias”* (sublinhado nosso).

Assim, e como consagrado no artigo 16.º da Diretiva (UE) 2019/1937, há uma obrigação de garantir a confidencialidade da identidade dos denunciantes.

Para além disto, determina o artigo 17, n.º 3 da Proposta de Lei n.º 91/XIV que: *“Salvo consentimento expreso do denunciante, a identidade deste só é divulgada em decorrência de obrigação legal ou decisão judicial”* (sublinhado nosso).

E de acordo com o artigo 17, n.º 4 da Proposta: *“Sem prejuízo do disposto em outras disposições legais, a divulgação da informação é precedida de comunicação escrita ao denunciante indicando os motivos da divulgação dos dados confidenciais em causa, exceto se a prestação dessa informação comprometer as investigações ou processos judiciais relacionados”*.

É de referir que resulta do artigo 26, n.º 1, alínea c) da Proposta que constitui contraordenação muito grave, sem prejuízo de eventual responsabilidade penal, o não cumprimento do dever de confidencialidade previsto no artigo 17.º.

Finalmente, determina o artigo 18.º da Proposta que os dados pessoais tratados ao abrigo da Proposta de Lei, observam o disposto no Regulamento de Proteção de Dados.

Como expressamente referido na Exposição de Motivos da Proposta de Lei n.º 91/XIV, em razão da matéria, e em sede de procedimento legislativo que decorreu na Assembleia da República, terão sido ouvidos o Conselho Superior da Magistratura, o Conselho Superior do Ministério Público, o Conselho Superior dos Tribunais Administrativos e Fiscais, a Ordem dos Advogados, a Associação Nacional de Municípios Portugueses, a Associação Nacional de Freguesias, os órgãos de governo próprio das Regiões Autónomas, a Autoridade de Supervisão de Seguros e Fundos de Pensões, o Banco de



Portugal, a Confederação Empresarial de Portugal, a Comissão do Mercado dos Valores Mobiliários, a Comissão Nacional de Proteção de Dados e a Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo.

Ora, tendo presente que a Assembleia da República será dissolvida pelo Presidente da República, nos termos do disposto na alínea e) do artigo 133.º da CRP, e por forma a obviar a que a Comissão pudesse dar início a um processo por infração e intentar uma ação contra o Portugal junto do Tribunal de Justiça da UE, a Assembleia da República, na última dia desta Sessão Legislativa, e depois de ter acordado em Conferência de Líderes uma versão nova da Proposta de Lei, fê-la aprovar neste dia 26 de novembro de 2021.

#### **4. Conclusão**

A corrupção e a fraude constituem, numa economia globalizada, um fenómeno de carácter transnacional e multidimensional com dimensões políticas, económicas, sociais e culturais, que mina as sociedades e as economias, enfraquece os Estados e as democracias.

Pela relevância que assumem no plano internacional e pelo impacto que projetam, várias têm sido as instâncias que se têm focado no desenvolvimento da prevenção e na luta contra a corrupção, nomeadamente, a Organização das Nações Unidas que aprovou de 31 de outubro de 2003 a Convenção das Nações Unidas contra a Corrupção.

Porém, se por um lado há que combater a corrupção com firmeza, por outro lado, e com igual determinação, há que proteger os direitos fundamentais daqueles que denunciem situações lesivas do interesse público.

Nessa medida, a União Europeia tem vindo a construir um edifício jurídico com a mesma robustez do existente para o combate à fraude e à corrupção, no qual assume especial relevância a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União e que terá de ser transposta para os Ordenamentos Jurídicos internos até ao dia 17 de dezembro de 2021.

No plano nacional, a Assembleia da República os aprovou, a 26 de novembro de 2021, a Proposta de Lei n.º 91/XIV que visa a transposição da Diretiva (UE) 2019/1937 para o ordenamento jurídico interno.

Os denunciantes assumem um papel central na descoberta, investigação e prevenção das infrações cometidas no contexto profissional e podem, deste modo, ser fundamentais para o combate à fraude. Deste modo, espera-se que tanto agora como no futuro seja reforçado, nos planos europeu e nacional, a privacidade e confidencialidade da identidade dos denunciantes, permitindo, deste modo, que estes se sintam seguros para denunciar as infrações cometidas dentro das organizações jurídicas em que laboram.



## 5. Bibliografia

BRANDÃO, Nuno – O *Whistleblowing* no ordenamento jurídico português, Lisboa: Revista do Ministério Público 161: janeiro: março 2020.

DE PITTA SIMÕES, Patrick – O *Whistleblowing* é um assunto de Polícia (s)?, Lisboa: Cedis Working Papers, setembro 2020.

SALDANHA, Nuno – RGPD – Guia para uma Auditoria de Conformidade -Dados, Privacidade, Implementação, Controlo, Compliance; Lisboa: FCA – Editora de Informática, Lda, junho de 2019.

## Legislação

### Nacional

Constituição da República Portuguesa. Disponível Online <https://dre.pt/legislacao-consolidada/-/lc/34520775/view>

Lei 19/ 2008, de 21 de abril - Aprova medidas de combate à corrupção e procede à primeira alteração à Lei n.º 5/2002, de 11 de janeiro, à décima sétima alteração à lei geral tributária e à terceira alteração à Lei n.º 4/83, de 2 de abril. Disponível em <https://dre.pt/pesquisa/-/search/249976/details/maximized>

Resolução do Conselho de Ministros n.º 37/2021, de 4 de junho de 2021, Disponível Online <https://dre.pt/home/-/dre/160893669/details/maximized>

Proposta de Lei n.º 91/XIV. Disponível Online <https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765247396a6457316c626e527663306c7561574e7059585270646d45764d7a4d7a595451344d546b744d47466a596930304e6a4a6b4c54686c597a55744d6a45325a6d566b4e546b314e545a6b4c6d52765933673d&fich=333a4819-0acb-462d-8ec5-216fed59556d.docx&Inline=true>

## Europeia

### Conselho da Europa

Convenção Europeia dos Direitos do Homem. Disponível Online [https://www.echr.coe.int/documents/convention\\_por.pdf](https://www.echr.coe.int/documents/convention_por.pdf)

### União Europeia

Carta de Direitos Fundamentais da União Europeia. Disponível Online <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>

Tratado de Funcionamento da União Europeia. Disponível Online [https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC\\_3&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF)

Tratado da União Europeia. Disponível Online [https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF)

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível Online <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046>

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível Online <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680>

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível Online <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>

Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725>

Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União. Disponível Online <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L1937&from=en>

### **Internacional**

Declaração Universal dos Direitos Humanos, disponível em <https://dre.pt/declaracao-universal-dos-direitos-humanos>

Convenção das Nações Unidas contra a Corrupção, disponível em <https://dre.pt/application/dir/pdf1sdip/2007/09/18300/0669706738.PDF>

Pacto sobre os direitos civis e políticos, disponível em [https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto\\_internacional\\_sobre\\_os\\_direitos\\_civis\\_e\\_politicos.pdf](https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto_internacional_sobre_os_direitos_civis_e_politicos.pdf)

---

# O “Espírito Dominicano” no Pensamento Político-Constitucional Ocidental: Algumas Notas<sup>147</sup>

Pedro Rebelo Botelho Alfaro Velez<sup>148</sup>

## RESUMO

O artigo versará sobre o significado no e para o pensamento político-constitucional ocidental da teoria político-jurídica produzida no seio da ordem dominicana. Sugeriremos e tentaremos ilustrar os seguintes tópicos fundamentais: i) O pensamento dominicano repropõe/repropõe o político-jurídico como “estrutura” com densidade própria positiva, tida como decorrente da ordem da criação; concretamente, como o lugar da vida boa, da vida virtuosa, e da ordem justa. ii) A teoria político-jurídica dos pregadores achou-se outrossim associada a uma tentada combinação da referida perspectiva (aristotélica-)tomista objectivista com uma compreensão mais enfaticamente “subjectiva” do político-jurídico em termos de direitos naturais. iii) Uma matriz político-jurídica de filiação dominicana foi e tem sido chamada à colação como base de construção e desenvolvimento da chamada doutrina social da Igreja, bem como de um projecto que aí se foi afirmando de transfiguração (de acolhimento mas também de superação) da gramática jurídico-política moderna, designadamente da subjectivista concepção de direitos humanos que a caracteriza esta última.

## PALAVRAS-CHAVE

tomismo; segunda escolástica; doutrina social da Igreja; direito natural; direitos humanos; direito constitucional.

---

<sup>147</sup> O presente texto corresponde a uma comunicação apresentada no Congresso internacional *Os Dominicanos no mundo luso-hispânico, história, arte e património*, que teve lugar na Sociedade de Geografia de Lisboa, de 23 a 26 de Julho de 2014, indicando-se a bibliografia então consultada. Sem prejuízo de uma sua ulterior publicação nas atas do evento, antecipamos a sua publicação nesta sede, com autorização dos Professores Doutores Fernando e Madalena Larcher, organizadores do referido Congresso. Agradeço penhoradamente à Senhora Professora Doutora Madalena Larcher a generosa revisão de texto a que pôde proceder.

<sup>148</sup> 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 políticoconstitucional e o religioso.

---

# The “Dominican Spirit” in Western Constitutional-Political Thought: Some Notes

*Pedro Rebelo Botelho Alfaro Velez*

## **ABSTRACT**

The article will deal with the meaning in and for the western political-constitutional thought of the political-legal theory produced within the Dominican order. We will suggest and try to illustrate the following key topics: i) Dominican thought re-proposed/re-proposes the political-juridical as a “structure” with its own positive density, seen as arising from the order of creation; concretely, as the place of the good life, the virtuous life, and the just order. ii) The political-juridical theory of the preachers’ order was/is also associated with an attempted combination of the aforementioned (Aristotelian-)Thomist objectivist perspective with a more emphatically “subjective” understanding of the political-juridical in terms of natural rights. iii) A political-juridical matrix of Dominican affiliation was foundational in the construction and development of the Church’s so-called social doctrine, namely in an exercise of transfiguration (an objectivist transformation) of the modern subjectivist juridical-political grammar and the contemporary human rights discourse.

## **KEYWORDS**

Thomism; scholasticism; social doctrine of the Church; natural law; human rights; constitutional law.

## Introdução

O que se pode e deve dizer de um ponto de vista teórico-constitucional e jurídico-político, a perspectiva que nos sentimos habilitados a adoptar, sobre o significado no e para o pensamento político-constitucional ocidental da teoria político-jurídica produzida no seio da ordem dominicana?

Tentaremos ilustrar as seguintes ideias chave:

Que o pensamento dominicano repropôs/repropõe o político-jurídico como “estrutura” com densidade própria positiva, tida como decorrente da ordem da criação; concretamente, como o lugar da vida boa, da vida virtuosa, e da ordem justa.

Que na teoria político-jurídica dos pregadores talvez se ache também uma tentativa de combinar a referida perspectiva (aristotélica-)tomista objectivista sobre o político-jurídico com uma compreensão mais enfaticamente “subjectiva” do político-jurídico em termos de direitos naturais.

Que uma matriz político-jurídica de filiação dominicana foi e tem sido chamada à colação como base de construção e desenvolvimento da chamada doutrina social da Igreja, bem como de um projecto que aí se foi afirmando de *transfiguração* (de acolhimento mas também de superação) objectivista da gramática jurídico-política moderna, designadamente da específica e subjectivista concepção de direitos humanos que a acompanha.

### 1. A original gramática metafísico-política dominicana e o seu significado

O pensamento dominicano operou uma re-teorização, em âmbito cristão, do político-jurídico como *estrutura* com densidade própria positiva: como o lugar, decorrente da ordem da criação, da vida boa, da vida virtuosa, e da ordem justa.

No esquema teológico-político agostiniano, a comunidade política é pensada, ou pelo menos é sobretudo pensada, como decorrência do pecado. Evoca-se, aliás, a narração bíblica nos termos da qual a primeira cidade fora fundada por Caim.

Segundo S.Tomás, (re)lendo Aristóteles, a comunidade política tem origem na natureza intrinsecamente social e política do homem. O próprio Adão antes da Queda exerceria naturalmente um poder de governo (ainda que não coercivo)<sup>149</sup>.

O fim imediato da comunidade política é a vida boa, a vida virtuosa (a “substância” do bem comum). Pode ler-se no *De Regno*:

“[...] Videtur autem finis esse multitudinis congregatae vivere secundum virtutem. Ad hoc enim homines congregantur ut simul bene vivant, quod consequi non posset unusquisque singulariter vivens; bona autem vita est secundum virtutem; virtuosa igitur vita est congregationis humanae finis./It is, however, clear that the end of a multitude gathered together is to live virtuously. For men form a group for the purpose of living well together, a thing which the individual man living alone could not attain,

<sup>149</sup> John MILBANK, “The Gift of Ruling: Secularization and Political Authority”, em *New Blackfriars*, v.85 (2004), p.229.

and good life is virtuous life. Therefore, virtuous life is the end for which men gather together [...]<sup>150</sup>.”

Em última instância a comunidade política ordena-se a Deus (tal é o seu fim último). Segundo S.Tomás:

“Sed quia homo vivendo secundum virtutem ad ulteriorem finem ordinatur, qui consistit in fruitione divina, ut supra iam diximus, oportet eundem finem esse multitudinis humanae qui est hominis unius. Non est ergo ultimus finis multitudinis congregatae vivere secundum virtutem, sed per virtuosam vitam pervenire ad fruitionem divinam./Yet through virtuous living man is further ordained to a higher end, which consists in the enjoyment of God, as we have said above. Consequently, since society must have the same end as the individual man, it is not the ultimate end of an assembled multitude to live virtuously, but through virtuous living to attain to the possession of God<sup>151</sup>.”

Na comunidade política, as leis e o direito devem instanciar (no terreno delimitado pela virtude da justiça) a *lex naturalis*<sup>152</sup>, os imperativos racionais acerca dos bens perfectivos da natureza humana criada por Deus, com a sua ordem de inclinações naturais<sup>153</sup>. E devem reflectir também a lei divina, a qual não deixa também de *recordar* a lei natural – através dos 10 mandamentos, por exemplo. Tal permitirá a vida virtuosa e concorrerá para a fruição do que é tido como o Bem Supremo para os seres humanos.

Note-se que, apesar da mencionada base aristotélica, não deixa de haver um conjunto de teses aristotélicas que S.Tomás afasta. O pensamento político de S.Tomás pode também ser decodificado como uma empresa de correcção-aperfeiçoamento do pensamento de Aristóteles. A realização, a perfeição e a felicidade humanas transcendem definitivamente os âmbitos da *polis* e da política, com isso se superando tensões, impasses e ambivalências no *sistema* aristotélico<sup>154</sup>. Num quadro de uma teologia de *Imago Dei*, são postas de lado ideias como as de diferenciação qualitativa no humano entre os helenos (capazes de comunidade política) e o resto e de sacrifício de certas categorias de seres humanos mais frágeis à possibilidade de existência de Cidade<sup>155</sup>.

---

<sup>150</sup> *De Regno*, Livro I, cap. 15, §.º 106.

<sup>151</sup> *De Regno*, Livro I, cap. 15, §.º 107.

Ver Thomas AQUINAS, *De regno, ad regem Cypri/On kingship, to the king of Cyprus*, traduzido por Gerald B. Phelan e revisto por I.Th.ESCHMANN, O.P., The Pontifical Institute of Mediaeval Studies, Toronto, 1949; disponível em <https://www.dhspriory.org/~dhsprior/thomas/DeRegno.htm> (Re-edited and chapter numbers aligned with Latin, by Joseph Kenny, O.P.).

<sup>152</sup> Na síntese de John MILBANK: “Aquinas does place ius as dialectically arrived-at equity above lex seen as posited and formulated disposition expressing such equity: “right is the object of justice” says Aquinas, and “law is not the same as right but an expression of right” (ST 2.2 q.57 a.1 resp. and ad 2)” – “Against Human Rights: Liberty in the Western Tradition”, em *Oxford Journal of Law and Religion*, v.1, n.º 1 (2012), p.219-220.

<sup>153</sup> Sem querer aqui entrar em querelas interpretativas contemporâneas. Actualmente, nos círculos tomistas, certas interpretações da lei natural priorizam a razão prática enquanto “estrutura” autónoma (G. Grisez e J. Finnis, o movimento da *new natural law*), outras a noção metafísica de natureza humana (R. McInerney, R. Hittinger, E. Feser).

<sup>154</sup> Sobre o pensamento metafísico-político de Aristóteles vide a segunda parte de Eric VOEGELIN, *Order and History*, v.III, *Plato and Aristotle*, editado e introduzido por Dante Germino, University of Missouri Press, Columbia and London, 2000.

<sup>155</sup> Não podendo o universo dos cidadãos deixar de ser *estruturalmente* limitado a uns certos milhares, tal *solicitaria* várias medidas eugénicas....



A essência da *gramática* metafísico-política elaborada por S.Tomás pode ser melhor apreendida se a contrastarmos com a estrutura profunda da forma dominante de pensamento político-constitucional moderno. O que possibilitará, aliás, em sentido inverso, um olhar iluminante sobre esta última como destaque da gramática tomista...e, vê-lo-emos, como estrutura derivada de um certo fundo metafísico-político franciscano.

Desde logo, há que ter presente a descontinuidade entre a interpretação clássica-tomista do direito natural e as teorias dos direitos naturais de Hobbes, Locke, e também de Rousseau<sup>156</sup>. Tais teorias *interpretam* o homem como ser naturalmente apolítico, como ser dotado de uma liberdade concebida como desligada de um *telos* substantivo (do *Summum Bonum* clássico-católico), como um proprietário de si próprio. A sociedade política emerge, por *necessidade* de auto-preservação e/ou de *segurança* individuais, para garantir a coexistência de liberdades originárias indiferentes.

Estas ideias de ordem afirmar-se-iam definitivamente na cultura pública e política ocidental com as grandes revoluções inglesa, americana e francesa. O fenómeno das declarações de direitos manifesta-o eloquentemente – por elas as sociedades se instituem *ex novo* por referência a uma Lei tendo como aspecto nuclear uma noção de (*éga*)*liberté* entendida como “realidade” natural-individual negativa, i.é., sem uma regra substantiva intrínseca (como tem vindo a lembrar o jusfilósofo italiano Danilo Castellano).

Nos últimos decénios, uma tal matriz terá sido actualizada em grau superlativo: uma noção de (igual) liberdade individual, concebida como possibilidade de cada um escolher a sua concepção de bem (como poder de escolha auto-referencial e autotélico), parece mesmo tender a cristalizar como um Absoluto. A compreensão de liberdade que o Supremo Tribunal Americano celebrizou (caso *Planned Parenthood of Southeastern Pennsylvania v. Casey* 1992) parece ser disso sinal: “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”.

Na senda de pistas sugeridas por autores como Michel Villey, André de Muralt e John Milbank, parece ser de reconhecer que o *ethos* jurídico-público hoje dominante emergiu/emerge num espaço metafísico-político aberto pela revolução cosmovisional escotista-occamista<sup>157</sup>. Um espaço caracterizado pela ruptura com a essência da metafísica clássica-tomista e com a essência da metafísica política tomista: nesse

---

<sup>156</sup> Sobre estas últimas ver, por todos, Leo STRAUSS, *Natural Right and History*, The University of Chicago Press, Chicago/London, 1953; Paperback edition 1965. Ver também especificamente sobre Locke Juan Fernando SEGOVIA, *La ley natural en la teleraña de la razón: Ética, derecho y política en John Locke*, Marcial Pons, Madrid/Barcelona/Buenos Aires/São Paulo, 2014.

<sup>157</sup> Ver John MILBANK, “Against Human Rights: Liberty in the Western Tradition”, em *Oxford Journal of Law and Religion*, cit., p.203-234; André de MURALT, *L’unité de la philosophie politique. De Scot, Occam et Suárez au libéralisme contemporain*, Vrin, Paris, 2002; Michel VILLEY, “La genèse du droit subjectif chez Guillaume d’Occam”, em *Archives de Philosophie du Droit*, 9 (1964), p.97-127 e *La Formation de la Pensee Juridique Moderne*, Presses Universitaires de France, Paris, 2006.

espaço, Deus é compreendido em termos de uma vontade divina absoluta que se não caracteriza por uma ordem intrínseca; na estrutura da realidade não se reconhecem universais e essências. Analogicamente, a liberdade humana aparece como *quid* virtualmente desligado de um *telos*; como liberdade indiferente/indeterminada/não finalizada a que Deus apõe arbitrariamente um conjunto de normas-comandos extrínsecos.

É neste contexto que primeiro pôde aparecer a figura do direito subjectivo (Occam) – *potestas, facultas, libertas* do indivíduo humano sem referência a um *telos* ou uma teleologia.

Dáí em certo sentido se tenha podido afirmar que para a compreensão do pensamento político-constitucional moderno *normal*, na(s) sua(s) estruturas profundas e nas suas dinâmicas, mais do que uma contraposição entre antigos e modernos ou medievais e modernos, se afigure mais significativa, porque mais primária e mais originária, a dualidade espírito dominicano/espírito franciscano.

## **2. Uma (alter-)modernidade dominicana?**

Em S.Tomás, o direito é concebido objectivisticamente como *id quod iustum est* – como aquilo que é justo; como justo concreto, apurado por referência a um contexto relacional-posicional-societário (tidas em conta as instruções da lei natural). Não obstante, na obra do santo talvez se possa reconhecer a presença de um momento de uma compreensão outra do direito. Desde logo, S.Tomás parece afirmar a existência de certos direitos–garantias directamente ligados à dignidade da natureza humana enquanto tal: a garantia de não ser condenado sem julgamento e a de o ser por quem detém autoridade legítima, por exemplo. Para o santo existiriam ainda direitos-garantias ligados à dignidade do indivíduo humano como tal: ser julgado individualmente e não colectivamente<sup>158</sup>. Não se reconhece, porém, no corpus tomista, uma concepção de direitos subjectivos, se por direito subjectivo se entender uma *facultas agendi* humana-individual indiferente a um *telos* ou uma teleologia.

Na fileira dominicana da chamada segunda escolástica, cristaliza e torna-se especialmente visível no pensamento jurídico-político ocidental uma aproximação ao jurídico-político, a qual, não deixando de reivindicar filiação na (objectivista-teleológica) compreensão tomista do *ius (naturale)*, se apresentou como de índole mais subjectiva, interpretando o direito em termos de direitos-faculdades individuais. Um pretendido desenvolvimento a que não terá sido estranha a progressiva formação de

---

<sup>158</sup> Ver José Miguel Gamba, *La noción clásica de dignidad y los derechos humanos*, em *Anales de la Fundación Francisco Elías de Tejada*, Nº. 16, 2010, p.48 e nota 58.

um campo semântico em torno da ideia de direitos-faculdades que se foi apurando a partir do século XII, maxime no discurso jurídico-canónico<sup>159</sup>.

A definição vitoriana – Francisco de Vitoria (1483-1546), fundador da Escola de Salamaca – do ius como “potestas vel facultas conveniens alicui secundum leges/potestad o facultad que conviene a alguien según la ley<sup>160</sup>” disseminou-se entre os escolásticos do século XVI<sup>161</sup>. Segundo o dominicano Domingo de Soto (1495-1560), por exemplo,

“[...] jus idem est quod facultas disponendi de rebus liberique illis utendi/derecho es lo mismo que la facultad de disponer de las cosas y de usarlas libremente”<sup>162</sup>.

No parecer de alguns (Brian Tierney, designadamente), Vitoria, de Soto e Bartolomé de las Casas (1474-1566) teriam mesmo concebido os seres humanos como detentores de direitos naturais individuais-universais, dada a sua comum natureza de seres criados à imagem de Deus (imago Dei), isto é, enquanto seres capazes de razão, de uma razão que participa da Ratio Divina. Em tais moldes, ou pelo menos também em tais moldes, parece, se terá concebido e defendido o domínio dos índios sobre as suas terras e organizações políticas. A noção de direitos naturais – direitos-faculdades tidos como decorrentes da natureza humana – que se foi definindo no decurso dos séculos XII e XIII, maxime no discurso jurídico-canónico, teria aqui sido recolhida e aperfeiçoada.<sup>163</sup>

No que diz respeito à nova vaga do pensamento dominicano, caberá discutir: se ou até que ponto propôs ou prefigurou um conceito de direitos humanos (direitos universais do homem enquanto homem); se ou em que medida escapou a um conceito de direito subjectivo e de direitos subjectivos em sentido moderno individualista-possessivo e ateleológico; se ou até que ponto integrou harmonicamente os registos discursivos jurídico-políticos objectivista e (mais) subjectivo nela simultaneamente

---

<sup>159</sup> Ver Alejandro GUZMAN BRITO, “Historia de la denominación del derecho-facultad como “subjectivo””, em *Revista de Estudios Histórico-Jurídicos*, n.º XXV (2003), p.407-443; disponível em <http://www.rehj.cl/index.php/rehj/article/view/386/363>.

<sup>160</sup> *Sth. Tom. Aquinat.* (1533 - 1535), in II<sup>o</sup> II<sup>ae</sup>, qu. 62, art. 1, 5.

<sup>161</sup> Alejandro GUZMAN BRITO, “Historia de la denominación del derecho-facultad como “subjectivo””, *cit.*, p.415.

<sup>162</sup> *De justitia et jure* (1553 - 1554), lib. IV, qu. 1, art. 1.

Continuando a seguir o que assinalou Alejandro GUZMAN BRITO, “Historia de la denominación del derecho-facultad como “subjectivo””, *cit.*, p.416.

<sup>163</sup> Veja-se, de Brian TIERNEY, “The Idea of Natural Rights-Origins and Persistence”, em *Northwestern Journal of International Human Rights*, v.2, n.º1, 2004, p.3-12 e *Natural Rights: Before and After Columbus/Fulton Lectures*, 1994. O domínio dos índios sobre as suas terras e organizações políticas não deixou de ser confirmado pela Igreja. Na Bula *Sublimis Deus*, que Paulo III promulgaria em 1537, afirmou-se explicitamente: “We define and declare by these Our letters (...) that, notwithstanding whatever may have been or may be said to the contrary, the said Indians and all other people who may later be discovered by Christians, are by no means to be deprived of their liberty or the possession of their property, even though they be outside the faith of Jesus Christ; and that they may and should, freely and legitimately, enjoy their liberty and the possession of their property; nor should they be in any way enslaved; should the contrary happen, it shall be null and have no effect”. Vide o texto em <http://www.papalencyclicals.net/Paul03/p3subli.htm>.

presentes; numa palavra, se ou até que ponto se manteve essencialmente ligada à matriz tomista a que sempre proclamou fidelidade<sup>164</sup>.

Por outro lado, inovadora foi também a concepção de ordem e relações internacionais que então emergiu, designadamente em Vitoria, como que vislumbrando, antes de Vestefália, um mundo pós-vestefaliano: a ideia de que a humanidade como um todo (a família humana com as suas comunidades políticas) se organiza numa *communitas orbis* partilhando um bem comum, no qual se inclui o *ius gentium*<sup>165</sup>.

No nosso tempo, Bento XVI invocaria (estrategicamente?) Francisco de Vitoria como “precursor das Nações Unidas”, e especificamente da chamada “responsabilidade de proteger”:

“O frade dominicano Francisco de Vitoria, justamente considerado precursor da ideia das Nações Unidas, tinha descrito esta responsabilidade como um aspecto da razão natural partilhada por todas as Nações, e como resultado de uma ordem internacional cuja tarefa era regular as relações entre os povos. Agora, como então, este princípio deve invocar a ideia da pessoa como imagem do Criador, o desejo de uma liberdade absoluta e essencial”<sup>166</sup>.

### **3. O(s) uso(s) do espírito metafísico-político dominicano na doutrina política católica contemporânea.**

É a partir do pensamento dominicano que pudemos circunscrever, *maxime* a partir da metafísica política tomista, que a doutrina social e política da Igreja se tem vindo a desenvolver desde Leão XIII.

É também a partir dessa base que se tem esboçado a linha de força que progressivamente se tornou dominante no magistério social e político papal: a tentativa de dissociar *intenções* político-constitucionais modernas, tidas como válidas, de certos pressupostos subjectivistas de derivação *franciscana*, reconduzindo-as a uma base objectivista-teleológica ou integrando-as num quadro objectivista-teleológico (e nisso as transfigurando e recriando)<sup>167</sup>. Ou, dito de outro modo, a tentativa de projectar a

---

<sup>164</sup> Segundo alguns autores, a escola de Salamanca prefiguraria e inauguraria mesmo o contemporâneo discurso sobre os direitos humanos (Pedro CALAFATE). Para outros, prefiguraria e inauguraria sobretudo o contemporâneo e específico discurso católico sobre os direitos humanos (Paolo G. CAROZZA e Daniel PHILPOTT). No parecer de outros autores, em Vitoria e Las Casas reconhecer-se-ia apenas e meramente, também num plano formal de significantes, um discurso de *justiça objectiva e bem comum* (Juan VALLET DE GOYTISOLO). Segundo outros, estaria em causa, na segunda escolástica, um acolhimento do conceito de direito subjectivo e de direitos subjectivos em sentido moderno “individualista-possessivo” e ateleológico (M.VILLEY).

<sup>165</sup> Vide Eric VOEGELIN, *History of Political Ideas*, v.V: *Religion and the Rise of Modernity*, editado e introduzido por James L.WISERPP, University of Missouri Press, Columbia and London, 1998, p.108 e ss. (“Interpolity Relations Vitoria”). Em tema de Escola de Salamanca, e de “Escola Ibérica da Paz que dela brota”, veja-se agora Pedro CALAFATE e Ramón E.MANDADO GUTIÉRREZ (coordenadores), *Escola Ibérica da Paz/Escuela Ibérica de la Paz: a consciência crítica da conquista e colonização da América/La conciencia crítica de la conquista y colonización de América (1511-1694)*, Editorial de la Universidad de Cantabria e Real Sociedad Menéndez Pelayo, Santander, 2014.

<sup>166</sup>[http://www.vatican.va/holy\\_father/benedict\\_xvi/speeches/2008/april/documents/hf\\_ben-xvi\\_spe\\_20080418\\_un-visit\\_po.html](http://www.vatican.va/holy_father/benedict_xvi/speeches/2008/april/documents/hf_ben-xvi_spe_20080418_un-visit_po.html).

<sup>167</sup> Segundo sintetizou recentemente o agora papa emérito Bento XVI: “Foi para “pôr o mundo moderno em contacto com as energias vivificadoras e perenes do Evangelho” (João XXIII, *Const.ap.Humanae salutis*, 3) que se fez o Concílio Vaticano II, no qual a Igreja, a partir de uma renovada consciência da tradição católica,

ordem liberal, na sua dimensão institucional e de *praxis* (abstracção feita dos seus princípios fundacionais tidos por ideológicos), a partir de premissas jusnaturalistas católicas<sup>168</sup>.

Ao nascente “direito novo” moderno, Leão XIII responderia positivamente, reactivando e desenvolvendo a visão tomista do político-jurídico, no quadro-maior de uma recuperação geral da doutrina de S.Tomás (encíclica *Aeterni Patris*, de 4 de Agosto 1879)<sup>169</sup>. O Pontífice reproporia a ideia tomista de uma Cidade natural e cristã-católica – *maxime* na Encíclica *Immortale Dei* (1 Novembro 1885) sobre a *constituição cristã dos Estados*<sup>170</sup>. Uma ideia posteriormente enriquecida com contributos de S. Pio X (a ideia de civilização cristã, evocada na carta *Notre charge apostolique* de 23/10/1910 – I, 11) e de Pio XI (a ideia de reinado social de Cristo, definida na encíclica *Quas Primas* de 11 de Dezembro de 1925<sup>171</sup>).

Sempre a partir da referida metafísica política, o papa receberia a moderna linguagem dos direitos – e particulares instâncias então centrais da mesma – reelaborando a sua substância. Leão XIII afirmaria especificamente a existência de um direito natural à propriedade privada (*Rerum Novarum*, 15 de Maio de 1891<sup>172</sup>), e porventura um direito geral de liberdade<sup>173</sup>. Os direitos reconhecidos como naturais aparecem, no entanto, como intrinsecamente ligados a Deus, ao bem comum, e a deveres. Em sede de juízo específico sobre as chamadas “liberdades modernas” proclamadas pela Revolução distinguia-se: enquanto reivindicações de faculdades subjectivas incondicionais e absolutas não poderiam ser aceites; concebidas enquanto liberdades civis temperadas por razões de bem comum seriam aceitáveis<sup>174</sup>.

---

assume e discerne, transfigura e transcende as críticas que estão na base das forças que caracterizaram a modernidade, ou seja, a Reforma e o Iluminismo. Assim a Igreja acolhia e recriava por si mesma, o melhor das instâncias da modernidade, por um lado, superando-as e, por outro, evitando os seus erros e becos sem saída”. Vide *Discurso do Papa Bento XVI, encontro com o mundo da cultura, Centro Cultural de Belém – Lisboa, Quarta-feira, 12 de Maio de 2010*:

[http://www.vatican.va/holy\\_father/benedict\\_xvi/speeches/2010/may/documents/hf\\_ben-xvi\\_spe\\_20100512\\_incontro-cultura\\_po.html](http://www.vatican.va/holy_father/benedict_xvi/speeches/2010/may/documents/hf_ben-xvi_spe_20100512_incontro-cultura_po.html).

<sup>168</sup> Sobre estas temáticas ver, por todos, Paolo G. Carozza e Daniel Philpott, *The Catholic Church, Human Rights, and Democracy: Convergence and Conflict with the Modern State*, em *Logos: A Journal of Catholic Thought and Culture*, v.15, n.º 3, 2012, p.15-43. Cfr. também: Joseph A. KOMONCHAK, *Vatican II and the encounter between Catholicism and liberalism*, em R.BRUCE DOUGLASS e David HOLLENBACH (ed.), *Catholicism and Liberalism, Contributions to American Public Philosophy*, Cambridge University Press, Cambridge, 1994, p.76-100.

<sup>169</sup> Disponível em [http://w2.vatican.va/content/leo-xiii/it/encyclicals/documents/hf\\_l-xiii\\_enc\\_04081879\\_aeterni-patris.html](http://w2.vatican.va/content/leo-xiii/it/encyclicals/documents/hf_l-xiii_enc_04081879_aeterni-patris.html)

<sup>170</sup> Disponível em [http://w2.vatican.va/content/leo-xiii/pt/encyclicals/documents/hf\\_l-xiii\\_enc\\_01111885\\_immortale-dei.html](http://w2.vatican.va/content/leo-xiii/pt/encyclicals/documents/hf_l-xiii_enc_01111885_immortale-dei.html).

<sup>171</sup> Ver [http://w2.vatican.va/content/pius-xi/it/encyclicals/documents/hf\\_p-xi\\_enc\\_11121925\\_quas-primas.html](http://w2.vatican.va/content/pius-xi/it/encyclicals/documents/hf_p-xi_enc_11121925_quas-primas.html).

<sup>172</sup> [http://w2.vatican.va/content/leo-xiii/pt/encyclicals/documents/hf\\_l-xiii\\_enc\\_15051891\\_rerum-novarum.html](http://w2.vatican.va/content/leo-xiii/pt/encyclicals/documents/hf_l-xiii_enc_15051891_rerum-novarum.html).

<sup>173</sup> O Pontífice relevaria ainda um “direito natural e primordial de todo o homem ao casamento” (*Rerum Novarum*, § 6.º), bem como um direito de associação, um direito a prover o próprio sustento.

<sup>174</sup> Ver parágrafo 42 da encíclica *Libertas* (20 de Junho de 1888). A referida encíclica pode ser encontrada em: [http://www.vatican.va/holy\\_father/leo\\_xiii/encyclicals/documents/hf\\_l-xiii\\_enc\\_20061888\\_libertas\\_en.html](http://www.vatican.va/holy_father/leo_xiii/encyclicals/documents/hf_l-xiii_enc_20061888_libertas_en.html).

Com o magistério do papa Pio XI e sobretudo com o do papa Pio XII<sup>175</sup>, o tema dos *direitos fundamentais da pessoa humana* – direitos decorrentes da sua «dignidade» transcendente e sempre inseparáveis de uma teleologia – torna-se um tópico central de desenvolvimento doutrinal.

Na célebre mensagem de Natal de 1944 (*Benignitas et humanitas*), Pio XII dissertaria sobre as condições de uma *verdadeira e sã democracia*. A ordem democrática deve ser uma ordem submetida à lei natural e à lei divina (deveria fundar-se “sobre os imutáveis princípios da lei natural e das verdades reveladas”). O conceito de povo, sujeito de uma autêntica democracia, que se acha aí presente – um povo orgânico ordenado representado por um corpo de legisladores virtuosos e dotado de uma real autoridade organizadora – é tributário dos traços essenciais do regime misto, popular temperado, sugerido por S.Tomás (no já mencionado *De Regno*)<sup>176</sup>.

A *Pacem in terris*<sup>177</sup> do papa João XXIII elaboraria de modo orgânico-sistemático um discurso católico sobre os direitos do homem, detendo-se na questão das suas bases ontológicas. Os direitos humanos fundam-se na natureza humana, não presumem uma apoliticidade natural, e, pelo menos em última análise<sup>178</sup>, são aspectos do/determinam-se em função do bem comum, exprimem uma teleologia substancial de carácter transcendente. Em tema de liberdade de espírito, os direitos naturais reconhecidos foram-no em termos de ligação originária à verdade e ao bem comum:

“Todo o ser humano tem [...] direito à liberdade na pesquisa da verdade e, dentro dos limites da ordem moral e do bem comum, à liberdade na manifestação e difusão do pensamento, bem como no cultivo da arte. Tem direito também à informação verídica sobre os acontecimentos públicos.<sup>179</sup>”

Na senda de Pio XII, sugere-se a existência de um direito à participação na *res publica*, interpretada também como serviço ao bem comum:

“Coere ainda com a dignidade da pessoa o direito de participar activamente da vida pública, e de trazer assim a sua contribuição pessoal ao bem comum dos concidadãos [...]”<sup>180</sup>.”

A referida encíclica exprimiria também uma aceitação qualificada de estruturas e formas constitucionalistas. FÁ-lo-ia *prudencialmente*, em nome de razões de bem

---

<sup>175</sup> Ver, por exemplo, o parágrafo 34.º da *Radiomensagem do Natal de 1942 (Con sempre nuova freschezza)* -[http://w2.vatican.va/content/pius-xii/pt/speeches/1942/documents/hf\\_p-xii\\_spe\\_19421224\\_radiomessage-christmas.html](http://w2.vatican.va/content/pius-xii/pt/speeches/1942/documents/hf_p-xii_spe_19421224_radiomessage-christmas.html).

<sup>176</sup> Ver *Radiomensagem Benignitas et humanitas às vésperas do Natal (24 de dezembro de 1944)* em: [http://w2.vatican.va/content/pius-xii/it/speeches/1944/documents/hf\\_p-xii\\_spe\\_19441224\\_natale.html](http://w2.vatican.va/content/pius-xii/it/speeches/1944/documents/hf_p-xii_spe_19441224_natale.html).

<sup>177</sup>Ver Carta encíclica *Pacem in Terris* (11 de abril de 1963): [http://www.vatican.va/holy\\_father/john\\_xxiii/encyclicals/documents/hf\\_j-xxiii\\_enc\\_11041963\\_pacem\\_po.html](http://www.vatican.va/holy_father/john_xxiii/encyclicals/documents/hf_j-xxiii_enc_11041963_pacem_po.html).

<sup>178</sup> De facto, lê-se no § 9.º «Em uma convivência humana bem constituída e eficiente, é fundamental o princípio de que cada ser humano é pessoa; isto é, natureza dotada de inteligência e vontade livre. Por essa razão, possui em si mesmo direitos e deveres, que emanam direta e simultaneamente de sua própria natureza. Trata-se, por conseguinte, de direitos e deveres universais, invioláveis, e inalienáveis.» (sublinhados nossos).

<sup>179</sup> § 12.º

<sup>180</sup> § 26.º



comum também alicerçadas numa interpretação da experiência histórica<sup>181</sup>. A um outro nível, algo de idêntico se poderia dizer quanto às normas estruturantes da nascente organização da comunidade internacional, *maxime* da Declaração Universal dos Direitos do Homem<sup>182</sup>. Na senda da teorização internacionalista iniciada por Vitoria, dada a que se entende ser a contemporânea configuração do bem comum universal, sugere-se que a ordem moral exigiria a instituição de uma autoridade pública universal que o pudesse, com efectividade, tomar como fim (sem deixar de respeitar os direitos da pessoa humana e um princípio de subsidiariedade)<sup>183</sup>.

O referido património piano e joanino seria recebido pelo Concílio Vaticano Segundo (1962-1965), *máxime* na *Gaudium et spes*.<sup>184</sup> Com a declaração *Dignitatis humanae*<sup>185</sup>, o concílio ensinaria mesmo um *novel* direito à liberdade religiosa: um direito natural à liberdade civil em matéria religiosa. Em certo sentido (num sentido formal-estrutural) análogo ao direito de idêntica denominação da tradição constitucionalista, receberia, porém, uma fundação *pré-moderna* objectivista e teleológica. Se bem que se tivesse podido afirmar no universo da teologia católica uma interpretação dessa declaração em termos de imunidade de coacção derivada de uma noção de dignidade humana sobretudo associada a uma ideia de autonomia (John Courtney Murray)<sup>186</sup>.

A partir de uma base *objectivista* de radicação tomista, João Paulo II desenvolveria o discurso católico sobre os direitos humanos, exprimindo-se o seu vasto ensinamento social fundamentalmente nessa matriz. A contraposição entre um discurso católico dos direitos humanos e as interpretações seculares dos direitos humanos torna-se eminentemente patente<sup>187</sup>. É que no primeiro os direitos humanos são tidos como “[...] direitos humanos universais, radicados na natureza da pessoa, nos quais se reflectem as exigências objectivas e invioláveis de uma lei moral universal” (para evocar o célebre discurso por ocasião do 50.º aniversário da UN, em 5 de Outubro de 1995)<sup>188</sup>.

---

<sup>181</sup> Lê-se no parágrafo 78.º da encíclica: “Certamente não se pode aceitar a doutrina dos que consideram a vontade humana, quer dos indivíduos, quer dos grupos, primeira e única fonte dos direitos e deveres dos cidadãos, da obrigatoriedade da constituição e da autoridade dos poderes públicos”.

<sup>182</sup> Pode ler-se no parágrafo 143.º: “Contra alguns pontos particulares da Declaração foram feitas objeções e reservas fundadas. Não há dúvida, porém, que o documento assinala um passo importante no caminho para a organização jurídico-política da comunidade mundial. De facto, na forma mais solene, nele se reconhece a dignidade de pessoa a todos os seres humanos, proclama-se como direito fundamental da pessoa o de mover-se livremente na procura da verdade, na realização do bem moral e da justiça, o direito a uma vida digna, e defendem-se outros direitos conexos com estes”.

<sup>183</sup> § 136.º e ss.

<sup>184</sup> Constituição pastoral *Gaudium et Spes sobre a Igreja no mundo actual* (7 de Dezembro de 1965): [http://www.vatican.va/archive/hist\\_councils/ii\\_vatican\\_council/documents/vat-ii\\_const\\_19651207\\_gaudium-et-spes\\_po.html](http://www.vatican.va/archive/hist_councils/ii_vatican_council/documents/vat-ii_const_19651207_gaudium-et-spes_po.html).

<sup>185</sup> A Declaração *Dignitatis Humanae sobre a liberdade religiosa* 7 de Dezembro de 1965 pode ser vista em [http://www.vatican.va/archive/hist\\_councils/ii\\_vatican\\_council/documents/vat-ii\\_decl\\_19651207\\_dignitatis-humanae\\_po.html](http://www.vatican.va/archive/hist_councils/ii_vatican_council/documents/vat-ii_decl_19651207_dignitatis-humanae_po.html).

<sup>186</sup> Cfr. David L. SCHINDLER, “Religious Freedom, Truth, and American Liberalism: another look at John Courtney Murray”, em *Communio*, 21 (1994), p.696-741.

<sup>187</sup> Sobre essa contraposição ver Gustavo ZAGREBELSKY, *El derecho dúctil, Ley, derechos, justicia*, trad., 10.ª ed., Editorial Trotta, Madrid, 2011, p.75 e ss.

<sup>188</sup> O referido discurso pode ser visto em: [http://www.vatican.va/holy\\_father/john\\_paul\\_ii/speeches/1995/october/documents/hf\\_jp-ii\\_spe\\_05101995\\_address-to-uno\\_it.html](http://www.vatican.va/holy_father/john_paul_ii/speeches/1995/october/documents/hf_jp-ii_spe_05101995_address-to-uno_it.html).



Sem contradizer a ideia, explícita em Leão XIII, segundo a qual nenhuma forma de governo possui em si própria validade absoluta sendo preferível em quaisquer circunstâncias, João Paulo II ensinaria explicitamente que “a Igreja encara com simpatia o sistema da democracia” (*Centesimus Annus*, 1991<sup>189</sup>). É elencada como justificação desse juízo a possibilidade de participação cidadã na vida política, ideia de radicação tradicional (*Quod omnes tangit...*) *atualizada*, já atrás encontrada. Sustenta-se, porém, que um tal sistema se deve basear numa “recta concepção da pessoa humana”, adoptando como “um autêntico e sólido fundamento” (o que se entende como) os direitos humanos (bem compreendidos)<sup>190</sup>. A democracia é entendida como “um ordenamento e, como tal, um instrumento, não um fim”; um ordenamento cujo “carácter moral não é automático, mas depende da conformidade com a lei moral, à qual se deve submeter como qualquer outro comportamento humano (...)” (*Evangelium vitae*, 1995<sup>191</sup>). Com base num tal paradigma, o pontífice diagnosticaria, focando atmosferas ideológicas e interpretações de certos direitos fundamentais, um afastamento das democracias realmente existentes em relação ao seu melhor conceito (“ideal democrático”) na direcção de “um substancial totalitarismo” e de um “Estado Tirano” (*Evangelium vitae*).

Bento XVI reenfatizaria a ideia de lei natural, repondo explicitamente a lei natural como base ontológica da ordem política, como substância do bem comum, como referente das leis positivas.

A esta luz revisitaria também o tópico do fundamento dos direitos humanos, “baseados na *lei moral natural* inscrita no coração do homem e presente nas diversas culturas e civilizações”, como “medidas do bem comum”, sublinhando o vínculo indissociável entre direitos e deveres e o primado destes últimos, explicitando que “da antropologia integral, que deriva da Revelação e do exercício da razão natural, dependem a fundação e o significado dos direitos e dos deveres humanos”<sup>192</sup>. Em tema de liberdade religiosa, Bento XVI aprofundaria a compreensão da mesma como liberdade fundada na dignidade humana entendida como capacidade de verdade e

---

<sup>189</sup> Ver a carta encíclica *Centesimus Annus* (1 de Maio de 1991) em [http://www.vatican.va/holy\\_father/john\\_paul\\_ii/encyclicals/documents/hf\\_jp-ii\\_enc\\_01051991\\_centesimus-annus\\_po.html](http://www.vatican.va/holy_father/john_paul_ii/encyclicals/documents/hf_jp-ii_enc_01051991_centesimus-annus_po.html).

<sup>190</sup> “[...] o direito à vida, do qual é parte integrante o direito a crescer à sombra do coração da mãe depois de ser gerado; o direito a viver numa família unida e num ambiente moral favorável ao desenvolvimento da própria personalidade; o direito a maturar a sua inteligência e liberdade na procura e no conhecimento da verdade; o direito a participar no trabalho para valorizar os bens da terra e a obter dele o sustento próprio e dos seus familiares; o direito a fundar uma família e a acolher e educar os filhos, exercitando responsabilmente a sua sexualidade. Fonte e síntese destes direitos é, em certo sentido, a liberdade religiosa, entendida como direito a viver na verdade da própria fé e em conformidade com a dignidade transcendente da pessoa”, nos termos da *Centesimus Annus*.

<sup>191</sup> [http://www.vatican.va/holy\\_father/john\\_paul\\_ii/encyclicals/documents/hf\\_jp-ii\\_enc\\_25031995\\_evangelium-vitae\\_po.html](http://www.vatican.va/holy_father/john_paul_ii/encyclicals/documents/hf_jp-ii_enc_25031995_evangelium-vitae_po.html).

<sup>192</sup> Ver *Discurso do papa bento xvi aos participantes na plenária do pontifício conselho «justiça e paz», sala do consistório, segunda-feira, 3 de dezembro de 2012*. [http://www.vatican.va/holy\\_father/benedict\\_xvi/speeches/2012/december/documents/hf\\_ben-xvi\\_spe\\_20121203\\_justpeace\\_po.html](http://www.vatican.va/holy_father/benedict_xvi/speeches/2012/december/documents/hf_ben-xvi_spe_20121203_justpeace_po.html).

transcendência. E também como liberdade a que é ínsita uma dimensão pública<sup>193</sup>. Estaria em causa aqui, segundo alguns, um retomar da compreensão antiga e medieval da liberdade, articulada com perfeição em S.Tomás, como sempre já direcionada à verdade e ao bem, à Verdade Primordial e ao Supremo Bem<sup>194</sup>.

Uma renovada atenção magistral ao conceito de laicidade – (re)descrito como “laicidade sadia” (retomando Pio XII) ou como “laicidade positiva” (adoptando-se um termo divulgado pelo presidente Nicolas Sarkozy) – apoiar-se-ia numa doutrina conciliar de reivindicada filiação tomista: na noção de legítima autonomia das realidades terrenas ou temporais enquanto realidades criadas<sup>195</sup>. Na ordem moral natural, estaria a fonte da consistência própria da esfera política distinta da esfera religiosa e da eclesial<sup>196</sup>. O cristianismo – em última análise o catolicismo enquanto *religio vera* – seria indispensável à construção da *polis*, na medida em que libertaria a razão de potenciais cegueiras éticas, permitindo uma apreensão plena da lei moral natural<sup>197</sup>.

O projecto católico de *transfiguração* (de acolhimento mas também de superação) objectivista da gramática jurídico-política moderna tem sido alvo de problematização, sendo questionada a sua consistência e coerência<sup>198</sup>. Seja qual for a valoração última que mereça o referido projecto, não sofre, porém, dúvida que o pensamento dominicano é ainda uma referência viva do/no pensamento político-constitucional ocidental.

---

<sup>193</sup> Ver Mensagem de sua Santidade Bento XVI para a celebração do XLIV dia mundial da paz (1 de janeiro de 2011): *Liberdade religiosa, caminho para a paz*, disponível em [http://www.vatican.va/holy\\_father/benedict\\_xvi/messages/peace/documents/hf\\_ben-xvi\\_mes\\_20101208\\_xliv-world-day-peace\\_po.html](http://www.vatican.va/holy_father/benedict_xvi/messages/peace/documents/hf_ben-xvi_mes_20101208_xliv-world-day-peace_po.html).

<sup>194</sup> Cfr. David L. Schindler, *Freedom, truth, and human dignity: an interpretation of dignitatis humanae on the right to religious liberty*, em *Communio*, 40, 2013, p.208 a 316.

<sup>195</sup> Modo de ver a laicidade sugerido já por Paulo VI. Ver Audiência Geral de 22 de Maio de 1968: [http://www.vatican.va/holy\\_father/paul\\_vi/audiences/1968/documents/hf\\_p-vi\\_aud\\_19680522\\_it.html](http://www.vatican.va/holy_father/paul_vi/audiences/1968/documents/hf_p-vi_aud_19680522_it.html).

<sup>196</sup> Atente-se no seguinte passo do Discurso do papa Bento XVI de 2 de junho de 2012: “[Por outro lado], na medida em que se ultrapassa a concepção de um Estado confessional, parece claro, contudo, que as suas leis devem encontrar justificação e força na lei natural, que é fundamento de uma ordem adequada à dignidade da pessoa humana, superando um conceito meramente positivista do qual não podem derivar indicações que sejam, de modo algum, de cunho ético...”. Disponível em: [http://www.vatican.va/holy\\_father/benedict\\_xvi/speeches/2012/june/documents/hf\\_ben-xvi\\_spe\\_20120602\\_autorita-milano\\_po.html](http://www.vatican.va/holy_father/benedict_xvi/speeches/2012/june/documents/hf_ben-xvi_spe_20120602_autorita-milano_po.html).

<sup>197</sup> Ver o parágrafo 28.º da Encíclica *Deus caritas est* (2005) [http://www.vatican.va/holy\\_father/benedict\\_xvi/encyclicals/documents/hf\\_ben-xvi\\_enc\\_20051225\\_deus-caritas-est\\_po.html](http://www.vatican.va/holy_father/benedict_xvi/encyclicals/documents/hf_ben-xvi_enc_20051225_deus-caritas-est_po.html).

<sup>198</sup> Para uma desconstrução de tal projecto como uma inviável combinação de opostos incomunicáveis, veja-se, por exemplo, Bernard DUMONT, Miguel AYUSO, Danilo CASTELLANO, *Iglesia y política, Combiar de paradigma*, Itinerarios, Madrid, 2013.

The background consists of numerous thin, wavy, layered lines in shades of pink and light red, creating a sense of depth and movement. The lines are stacked and curved, resembling a stack of paper or a liquid surface. The overall effect is a soft, textured, and dynamic visual field.

# II\_Outros Estudos

---

# A evidência digital na cadeia de custódia electrónica para incidentes CBRNE

Gabriel Pestana<sup>199</sup>

## RESUMO

Disponer de um registo padronizado sobre a custódia de evidências digitais para eventos do tipo CBRNE<sup>200</sup> é hoje uma questão crítica. A autenticidade da prova deve ser mantida desde o instante em que é identificada pela primeira vez, até que seja apresentada em tribunal. Isso significa que preservar a cadeia de custódia é seguir um procedimento padronizado para garantir a qualidade dos dados. O artigo aborda o processo de análise de evidências digitais, estabelecendo que cada item de evidência deve ser considerado da perspectiva de onde veio, quem o criou, quando, onde e por quê. Isso significa que a cadeia de custódia digital (dCoC) é estabelecida sempre que um dos atores (e.g., equipa de recolha, equipa de transporte e equipa no laboratório) assume a custódia da evidência digital. As diretrizes apresentadas, para o fluxo de trabalho (*workflow*) da dCoC, pretendem estabelecer um conjunto de boas práticas que devem ser adotadas em operações forenses, como parte dos procedimentos de trabalho, para realizar auditorias eficazes e confiáveis sempre que ocorra uma transferência de custódia.

## PALAVRAS-CHAVE

fluxo de trabalho na governação de dados, metadados sobre evidências digitais, contexto da alarmística, BPMN

---

<sup>199</sup> Gabriel Pestana é Professor e investigador sénior no projeto STATEGY, responsável pela coordenação de tarefas relacionadas com a criação de um *standard* de interoperabilidade para uma estrutura de dados (i.e., info-estrutura de metadados) relacionada com a Cadeia de Custódia Eletrónica para eventos do tipo CBRNE. Abordagem arquitetural assente na especificação de um *workflow* de governação de informação de suporte ao processo de decisão. (0000-0001-6916-2575). INOV - Institute of Systems and Computer Engineering Innovation Lisbon, Portugal, gabriel.pestana@inov.pt

<sup>200</sup> CBRNE um acrónimo para Chemical, Biological, Radiological, Nuclear, and Explosives.

---

# Digital Custody Transfer for CBRNE Events<sup>201</sup>

*Gabriel Pestana*

## ABSTRACT

Keeping a standardised record regarding the custody of digital evidence for CBRNE events is nowadays a critical issue, as the authenticity of evidence must be maintained following the condition when it was first discovered until later presented in the court. This means that preserving the chain of custody is about following a standardised procedure to ensure data quality. The paper steers the digital evidence examination process by providing that each item of evidence is to be considered from the perspective of where it came from, who created it, when, where, and why. This means that the digital chain of custody (dCoC) is established whenever the intervenient actors (e.g., collection team, carrier team and laboratory team) take custody of the digital evidence. The guidelines presented for the dCoC workflow aims to establish the essential practices to be followed by the participants in forensic operations as part of the work procedures required to perform effective and reliable auditing of custody transfer.

## KEYWORDS

data governance workflow, digital evidence metadata, context-awareness, BPMN

---

<sup>201</sup> Acknowledgements: the paper was developed within the scope of the STRATEGY project (H2020-EU.3.7-883520), an EU-funded research project to develop a pan-European framework of pre-standardisation activities for systems, solutions and procedures. It brings together standardisation bodies, policymakers, technology suppliers, and first responders from several EU countries who collaborate to improve interoperability between crisis management solutions within and between countries.



## Introduction

The term CBRNE is an acronym for Chemical, Biological, Radiological, Nuclear, and high yield Explosives is being used in both civilian and military organisations (ICRC, 2014). A CBRNE event refers to the uncontrolled release of chemicals, biological agents or radioactive contamination into the environment or explosions that cause widespread damage (Drury B., 2019). This means that CBRNE events can be caused by accidents or by terrorist acts. A CBRNE incident differs from a hazardous material incident in both scope (i.e., mass casualty situation) and intent (i.e., an event caused by an unintentional accident or with the specific intention of inciting terror or causing physical or environmental harm).

A hazardous material incident is usually associated with a safety emergency procedure, comprising a smaller-scale, accidental and non-weaponised event. A CBRNE incident is typically associated with an intentional attack and, therefore, classified as a security emergency procedure requiring the intervention of a Law Enforcement Agency or even the military's intervention (Heffelfinger D., 2013). Independently of the type of CBRNE event, the paper viewpoint is focused on representing the data governance workflow that needs to be implemented for the scene assessment by a forensic investigation team. In particular, the challenges related to digital scene surveying and risk assessment include identifying the resources assigned to a CBRNE mission. In addition, monitor who owns the custody at each step of the digital chain of custody (dCoC).

The main goal is to maintain the integrity of the information structure (i.e., the info-structure = electronic data and metadata of the Sample) throughout the investigation process, meaning the duration of the CBRNE mission. The digital record can be updated in various fashions, including direct computer inputs into the dCoC forms, establishing a synchronous communication with the intervenient teams and keeping the Mission Commander Team with a real-time update of the process execution (i.e., on-site scene forensic operations). Advantageously, the proposed dCoC was conceptualised to provide a valid token when communicating with any operational resource or external system. In this way, it becomes challenging to tamper with the data a user once stored. In this data governance workflow, existing SOPs do not cover in detail the critical situation of custody transfer. Each transfer point represents a vulnerability that might compromise the dCoC, requiring a standardised approach with a well-defined info-structure.

### 1. Discussion of the problem in digital investigation

In an investigation or judicial process, the physical and digital evidence is becoming an integral part of the investigation process. Thereby, the handling of physical or digital evidence is supposed to be the same or at least has a similar mechanism. The problem encountered these days is the gap in handling digital evidence, particularly in monitoring

digital custody. That is why it requires a framework for managing evidence that will support digital forensics operations.

Another problem related to digital evidence is the documentation. Documenting and recording all interactions on the physical evidence is easy to perform; however, this does not apply to digital evidence. The ease of remote access, copying, and transferring the file, coupled with the user mobility trend in daily activities, allows a digital investigator or other law enforcement agencies to explore and analyse the data anywhere and anytime as such requiring accurate data logs of the digital evidence with detailed information to support the investigation process. Signature of the object, identity of all parties who interact with the evidence, location of handling the evidence, time of access and all the descriptions that contain transactions and any access to the evidence would be required (Abbas T., 2018).

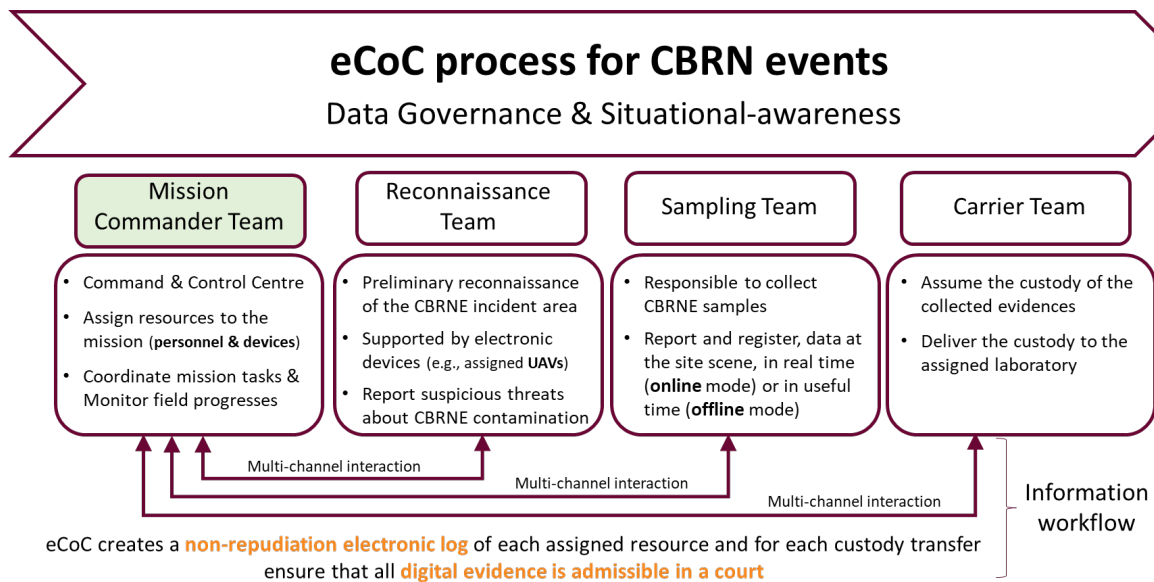
Within the scope of this paper, the dCoC refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of digital evidence in legal cases. Each step in the chain is essential as if broke (i.e., mishandling digital evidence), the digital evidence may be rendered inadmissible at court.

As presented in Figure 1, a close collaboration is required between the skilled actors and the Mission Commander, who has a complete and accurate grasp of the scope of the investigation. The diagram provides a workflow schema between participants to standardise the custody transfer data governance, triggering context-awareness whenever mishandling digital evidence is detected.

The Mission Commander Team enables speed, agility, and decisiveness at the tactical level while providing the necessary decision space at the higher level. They focus their orders on the purpose of the operation rather than on the details of how to perform assigned tasks. Participate in briefings and establish message control procedures. This means that a mission commander requires creative and skilful use of authority, instincts, intuition, and experience in decision-making and leadership to enhance operational effectiveness.

At the tactical level, reconnaissance, surveillance, security, and intelligence operations are the primary means a commander conducts information collection to answer the commander's critical information requirements to support decisive operations. At this level, the Reconnaissance Team is responsible for identifying and quantifying the threat (e.g., type of CBRNE agent involved) and documenting the scene. The next step is for the Sampling Team to collect priority forensic evidence (e.g., CBRNE samples at the site scene). The following step is for the Carrier Team to transport the evidence to its final destination to enable the subsequent analysis (e.g., the laboratory responsible for analysing the collected samples).





*Figure 1 Conceptual approach to the concept of dCoC.*

The diagram presents a high-level view of the workflow for tracking and recording digital evidence for assets within the chain of custody that creates a digital non-repudiation<sup>202</sup> log of each custody transfer at each transfer point from initial creation to final transfer or disposal. These combined processes are considered essential for effective network management and security (Giova G., 2016). Applying standard operating procedures (SOP) will contribute to a uniform description of the dCoC process, simultaneously clarifying the need for chronological documentation at each custody transfer point. The reported information must register all the evidence's details at every step in the dCoC workflow. Such a system must provide an answer to the following fundamental questions (5W1H):

- **What** is digital evidence (e.g., provide a fingerprint of digital evidence)?
- **Where** was digital evidence discovered, collected, handled and examined (e.g., GPS locations of the resource who handles evidence)?
- **Who** manages (make contact) with digital evidence (e.g., biometrics characteristics)?
- **Why** (reason) for using the digital evidence?
- **When** digital evidence custody is handled or transferred (e.g., provide a timestamp)?
- **How** is digital evidence used (e.g., specify the SOP adopted)?

One of the most sensitive variables in this workflow is the "time and moment of contact" with digital evidence. Knowing the current location of the evidence is not enough; there should be accurate logs tracking the movement and possession of evidence material at all times (Koleoso R., 2018). The integrity of eCoC plays a significant role in the digital process. In every phase, forensic investigators must know where, when, and how the digital evidence was discovered, collected, handled with, when, and who

<sup>202</sup> Non-Reputable, in computer security this concept refers to a transaction that can't be denied as having taken place or being legitimate.

came in contact with the evidence, etc. Proper dCoC must include documentation with answers to all these questions. If one of these questions remains unanswered, the chain of custody is compromised and disrupted. In this case, when presenting evidence in court, if one link were missing in the chain of evidence, the court would not accept the evidence as relevant.

## 2. Overview of the chain of evidence custody

Maintaining a proper chain of custody is essential to the one who preserves data, as well as authorities who may want to pursue legal action (Ćosić J., 2012). Keeping a standardised record regarding the custody of digital evidence had become a critical issue, as the authenticity of evidence must be maintained following the condition when it was first discovered until later presented in the court. The scope of the chain of custody includes all resources involved in the acquisition, collection, analysis of evidence, time records, and contextual information, which includes case labelling, and the unit and laboratory that process evidence.

The conventional approach for dCoC cannot be used to handle digital evidence due to the peculiar characteristics of digital evidence. Managing the chain of custody for digital evidence is more complex than handling physical evidence. It involves the recording metadata information and issues of access control and security for all the digital handling in the chain of custody (Prayudi Y. & Sn A., 2015). In this domain, the terms digital and electronic evidence are commonly used indistinctively; however, this is a mistake because each have a distinct scope:

- Digital evidence, i.e., any valuable information stored or transmitted in digital form or information stored or transmitted in a binary form that can be used in law enforcement and judicial processes (ENFSI, 2015).
- Electronic evidence has a physical form and can be identified visually (e.g., computer, mobile phone, camera, CD, hard disk, etc.). In contrast, digital evidence is extracted or recovered from electronic evidence (e.g., a file, email, short message, image, video, log, text).

Digital evidence is also very possible to cross countries and legal jurisdictions. For this reason, according to (Prayudi Y. & Ashari A., 2015), handling the chain of custody of digital evidence is much more complex than handling physical evidence, in general.

The dCoC process, presented in Figure 1, aims to establish the participants' essential practices when adopting an SOP that requires a standardised data governance workflow to monitor the digital evidence of custody transfer for CBRNE events. The transfer of data between participants is done using highly secure encryption algorithms (Alruwaili F., 2021). A formal Token must be generated at the Command and Control Centre to mitigate the risk of intrusions; for this to work, specific technologies such as Blockchain or Near Field Communication (NFC) may be considered. The adopted SOP must also assure multi-channel communications to simplify the interaction between the

Mission Command Team and other personnel at the site scene. Compliance with the authentication, authorisation, and accounting (AAA) framework is also recommended for intelligently controlling access to digital resources, enforcing policies and auditing related to the transfer of custody.

The main concern is to provide an info-structure of metadata to identify and track all resources (e.g., staff and equipment) allocated to a specific CBRNE mission, enabling all participants to clearly understand the requirements of digital evidence and its compliance with digital forensics operations. As such, the info-structure of metadata should provide information related to:

- Resources assigned to a specific CBRNE mission
- Create a digital record characterising a CBRNE sample
- Create a standardised digital log for each custody transfer (i.e., who owns the custody at each sample transfer point)
- Define a set of core indicators for assessing and monitoring the data workflow in the dCoC process (i.e., tracking CBRNE events, in particular, events related to the collected Sample)

We may conclude that the CBRNE mission requires careful response planning, which involves allocating multiple and highly qualified resources. Depending on the severity, specialised teams equipped with work-suits may be necessary to provide adequate protection during the operation in the contaminated area (i.e., sampling team). The diagram also outlines the information workflow that dCoC needs to implement between the identified Teams to ensure data governance, and most importantly, to keep all involved personnel well informed about the progress of CBRNE operations.

Data integrity is another issue in the dCoC (Prayudi Y. & Sn A., 2015); digital integrity is a property on which digital data do not experience any change by the party who is not authorised to do any change. Changes and contacts on digital evidence are only done by those who have the authority. The integrity of digital evidence warrants that the information presented is complete and unchanged from the first until used lastly in the court. As explained in Section 1, the necessity for the data integrity concept to ensure the handling of digital evidence is at the essence of any digital evidence management framework to obtain information that meets 5W1H.

### **3. An Overview of the Data Governance Process**

As presented in Figure 2, the flow chart outlines the workflow that needs to be implemented to represent the digital findings related to the CBRNE sampling process. The diagram describes the sequence of activities required to maintain the integrity of the data (and the corresponding metadata) throughout the dCoC process, especially when a change in custody is reported and when the data is accessible by different entities. Therefore, the main goal is to maintain the integrity of the information structure (i.e., the

data and the corresponding metadata associated with the participating actors' identification) throughout the investigation process (i.e., the CBRNE mission).

The BPMN<sup>203</sup> diagram corresponds to a formal representation of the workflow from the perspective of the Mission Commander, outlining the activities that are essential to keep the Mission Commander informed about the progress achieved by each actor within the dCoC. In addition, through this approach, it is possible to understand the importance of and the position of the chain of custody in digital forensics through a formal modelling approach.

The proposed workflow works the same way as a manual chain-of-custody (i.e., paper-based forms completed by hand). However, it offers critical benefits to help improve the chain of custody process, which can be operated in both modes: online and offline. The other difference resides in the fact that a typical dCoC speed up turnaround times by up to 25% and prevent common user errors associated with paper forms (Koleoso R.,2018). The direct benefits of implementing a dCoC include:

- Fewer data-entry and legibility issues with less paperwork to manage. The potential for data entry errors is reduced; information is entered into the system once, and the need to decipher handwritten information is eliminated;
- Eco-friendlier, as less paper is needed, eliminating the need for printing and shipping paper simultaneously. A QR code attached to every item accurately detail the corresponding information (e.g., Sample at the storage medium);
- Improved overall efficiency, quality, and accuracy by automating the storage and by having the informational artefacts pre-filled with data provided by the recognition team.
- Define an info-structure to mitigate the risk of intrusions, the possibility to verify all resources assigned to the mission and validate if the data token is valid for all incoming data.
- Reduced sampling site flaws by defining a set of standard actions that need to be in place. Such a higher quality process increases accuracy and reduces the cost;
- A significant decrease in affidavits and errors, improving turnaround time consequently as a result of electronic data availability;
- Labs receive pre-accessioned data that expedites laboratory analysis.

---

<sup>203</sup> A standard Business Process Model and Notation (BPMN) will provide businesses with the capability of understanding their internal business procedures in a graphical notation and will give organizations the ability to communicate these procedures in a standard manner. Furthermore, the graphical notation will facilitate the understanding of the performance collaborations and business transactions between the organizations, source OMG: [www.bpmn.org](http://www.bpmn.org).

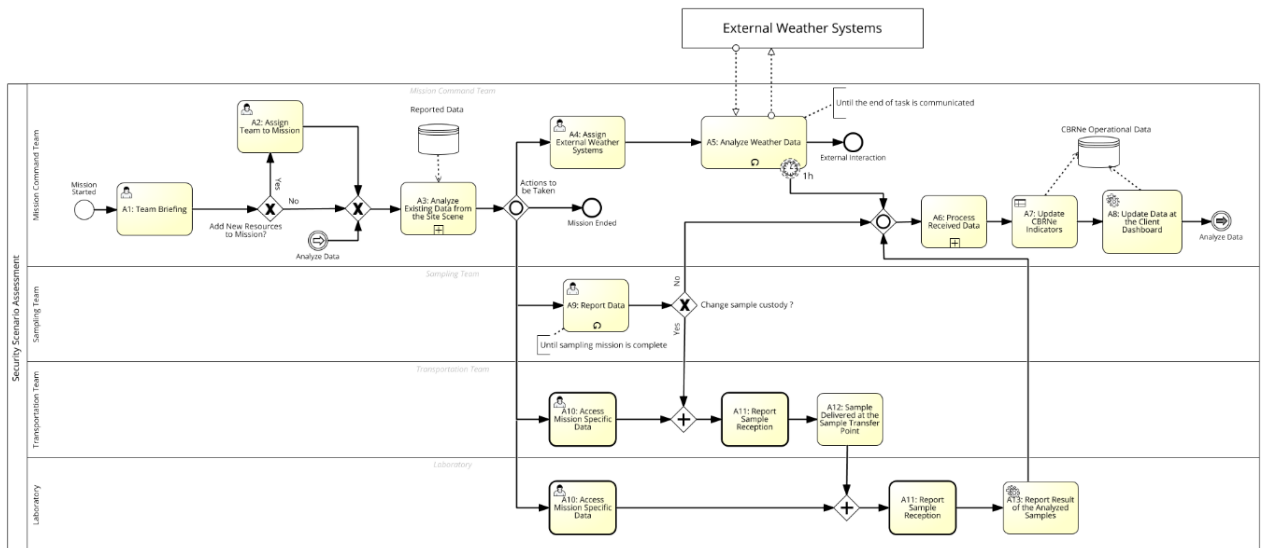


Figure 2 List of actors participating in data governance and reporting workflow for CBRNE events.

The proposed dCoC was conceptualised to provide a valid token when communicating with any operational resource or external system, keeping the Mission Commander Team with a real-time update of the process execution. In this way, it becomes challenging to tamper with the data a user once stored.

The most common way to build built-in token verification into the system is to introspect the token on the API Gateway and verify the signature on other services. In this introspection method, the token information usually includes token type, status (active or not), resource identifier, available scopes, expiration time, and any additional metadata required to assure the data authenticity. If we cannot add extra security functions on API Gateway, the token should be introspected on every service. Other token validation combinations are also possible under specific conditions; a particular choice between the methods should be made according to system architecture and security requirements. In this way, the system can validate the incoming data stream and then dispatch it to the correct storage area; alternatively, the data are redirected to a suspicious awareness log if any doubtful situation is detected.

#### 4. Conclusion and Further Research

The paper forwards the concept of digital chain of custody (dCoC), which is the process of verifying how digital evidence is collected, tracked, and protected on the way to the court. It guarantees that the data provided has not been tampered with and is true before being admitted as evidence. This is achieved by providing detailed information on how to process evidence at each step of the data governance workflow, focusing on the metadata needed to mitigate the risk of custody failure (error handling of digital evidence) at each custody transfer point, which may influence the court. Therefore, the most important thing for dCoC is to be able to store metadata information. The paper

also outlines the extent of the problems and challenges faced in the life cycle of digital evidence.

It also introduces the guidelines for the process and knowledge to be checked at each stage of the data governance workflow of the CBRNE incident, as well as the list of data and actions that should be included. Although this list does not pretend to be exhaustive, it outlines the scope of research that can contribute to dCoC. These guidelines aim to establish rules for digital forensics operations to ensure the integrity of the evidence and the evidence chain so that the evidence can be adopted in administrative, disciplinary and judicial procedures.

A BPMN diagram with a set of activities was presented as a contribution to standardising the data governance procedure based on a formal notation. Such an approach is a piece of clear evidence that the data governance workflow related to CBRNE events is feasible to be submitted for a standardised process. In this case, the collaboration diagram could map the process of analysing the severity level of a CBRNE incident, where an intentional release of a biological agent is masked as an outbreak.

The diagram also explains the role of each actor at each custody transfer point, outlining the need to keep a log of who owns the custody at each transfer point. These include knowing all the resources (human and equipment) assigned to the CBRNE mission and being involved in the digital evidence process. The info-structure of metadata will be able to answer the following questions: What is the digital evidence? Where is the digital evidence? Who manage with digital evidence? Why do it? When is digital evidence handled? How is dealt with digital evidence? These questions can be answered using fingerprints, biometrics, timestamp, GPS locators, a set of procedures, and best practices. Confidentiality in using the data and information acquired over an investigation is also subject of concern.

## 5. Reference

- Alruwaili, Fahad. (2021). CustodyBlock: A Distributed Chain of Custody Evidence Framework. *Information*. 12. 88. 10.3390/info12020088.
- Abbas, Talib. (2018). Adoption of Chain of Custody Improves Digital Forensic Investigation Process. *Iraqi Journal of Information & Communications Technology*. 1. 10.
- Ćosić, Jasmin & Ćosić, Zoran. (2012). Chain of custody and life cycle of digital evidence. *Journal of computer technology and application*.
- Drury, Brett & Ullah, Ihsan & Madden, Michael. (2019). An Information Retrieval System for CBRNe Incidents. 10.1007/978-3-030-13453-2\_17.
- ENFSI (2015). Best Practice Manual for Forensic Examination of Digital Technology. European Network of Forensic Science Institutes (ref. ENFSI-BPM-FIT-01).
- Giova, Giuliano. (2016). Digital Chain of Custody Quality Assessment. *International Journal of Computer Science and Network Security*. 16. 41-48.
- Heffelfinger, David & Tuckett, Craig & Ryan, Jeffrey. (2013). The Military's Response to Domestic CBRNE Incidents. *Journal of Homeland Security and Emergency Management*. 10. 10.1515/jhsem-2012-0013.
- ICRC (2014). Chemical, Biological, Radiological and Nuclear RESPONSE, introductory guidance for training purposes only. International Committee of the Red Cross, eBook.
- Koleoso, Rukayat. (2018). A Digital Forensics Investigation Model with Digital Chain of Custody for Confidentiality, Integrity and Authenticity. Thesis for PhD in Computer Science, School of Postgraduate Studies, University of Lagos.
- Krishnan, Sundar, and Shashidhar, Narasimha (2021). Interplay of Digital Forensics in eDiscovery. Proc. in the *International Journal of Computer Science and Security*, vol 15(2).
- Prayudi, Yudi & Ashari, Ahmad & Priyambodo, Tri. (2015). Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications*. 107. 975-8887. 10.5120/18781-0106.
- Prayudi, Yudi & Sn, Azhari. (2015). Digital Chain of Custody: State of The Art. *International Journal of Computer Applications*. 114. 975-8887. 10.5120/19971-1856.



A pair of glasses with dark frames is resting on an open book. The book's pages are filled with text, and the entire scene is overlaid with a semi-transparent pinkish-red filter. The background is a solid, light pink color.

# III\_Legislação e Jurisprudência Comentadas

---

# Comentário ao Acórdão do Tribunal da Relação de Coimbra relativo ao Processo 302/19.2T8MGL.C1, de 29 de junho de 2021

Lurdes Dias Alves<sup>204</sup>

## 1. O caso em análise

Em 29 de junho de 2021, o Tribunal da Relação de Coimbra (TRC) decidiu relativamente ao Processo 302/19.2T8MGL.C1<sup>205</sup> que, a empresa demandada agiu com licitude ao utilizar a imagem de um trabalhador numa revista publicitária e no respetivo website da empresa, com base no consentimento obtido de modo verbal e expresso do titular do direito à imagem, para a finalidade para a qual o consentimento foi obtido. O TRC confirmou a decisão recorrida, julgando improcedente o recurso.

## 2. Factualidade

Um motorista de uma empresa de transportes internacionais de mercadorias (*Um dos maiores grupos ibéricos de transportes*), que cessara funções ainda no decurso do período experimental<sup>206</sup>, recorreu a tribunal pedindo para que a empresa fosse impedida de utilizar a sua imagem e condenada a pagar-lhe uma indemnização.

Exigindo ainda que, a empresa fosse condenada a proceder à entrega de todas as cópias de documentos (*cópia do cartão de cidadão, carta de condução, cartão de qualificação de motorista, cartão de condutor (tacógrafo) cartão europeu de saúde, fotografia tipo passe, boletim de vacinas, fotocópia de cartão de cidadão da*

---

204 Licenciada em Direito e pela Universidade Autónoma de Lisboa. Pós-graduada em Direito Comercial e Direito Societário pela Universidade Católica Portuguesa – Escola de Lisboa. Mestre em Direito (especialidade de Ciências Jurídicas) pela Universidade Autónoma de Lisboa. Doutoranda em Direito (especialidade de Ciências Jurídicas) na Universidade Autónoma de Lisboa, onde investiga o tema: “A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade”. Investigadora integrada no RATIO LEGIS - Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa. Coordenadora de Pós-Graduações em: Proteção de Dados Pessoais, Privacidade e Cibersegurança na EU; e Prevenção e Detecção de Fraude Empresarial, na Autónoma Academy (Escola de Pós-graduações da Universidade Autónoma de Lisboa). Professora universitária convidada na Universidade Autónoma de Lisboa. Autora de várias publicações e participante regular em iniciativas públicas de Direito do trabalho e Proteção de Dados. Consultora Jurídica.

205 Acórdão do Tribunal da Relação de Coimbra de 29 de junho de 2021 (Proc.º 302/19.2T8MGL.C1). Relator: Desembargadora Sílvia Pires. [em linha]. Consultado em 9 de janeiro de 2022. Disponível em: <http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/141b49e56fb1bbc280258707003588fa?OpenDocument>

206 Salienta-se, para melhor análise e enquadramento, que, em 4 de dezembro de 2018 o autor e a ré celebraram, sob a forma verbal, um contrato de trabalho entre si; no âmbito do qual o autor se obrigou a desempenhar as funções de motorista de viaturas pesadas de âmbito nacional e internacional; O autor iniciou as funções no dia 7 de dezembro de 2018; tendo permanecido em formação até ao dia 27 de janeiro de 2019; no dia 22 de fevereiro de 2019 o autor e a ré acordaram o termo do vínculo laboral. Portanto, já na vigência do REGULAMENTO (UE) N.º 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. Jornal Oficial da União Europeia. (4.5.2016), 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).

*esposa), que se encontram na sua posse, bem como abster-se de os difundir, divulgar ou publicitar por qualquer forma.*

Com efeito, o facto em crise, fundava-se na utilização por parte da empresa de uma fotografia sua, captada durante o período de formação inicial, numa revista publicitária e no seu website.

A empresa contestou, alegando que o trabalhador tinha dado o seu consentimento para a captação da fotografia, sabendo que a mesma seria utilizada na revista e no site da empresa, e que nunca pretendia associar a imagem do autor à família deste, designadamente com o intuito de com isso obter algum benefício financeiro.

A ação foi julgada parcialmente procedente, com a condenação da empresa a apenas deixar de utilizar, no futuro, a imagem do trabalhador para fins publicitários ou outros de cariz comercial e com a condenação do trabalhador no pagamento de uma multa e indemnização como litigante de má-fé.

### **3. Apreciação do Tribunal da Relação de Coimbra**

- O direito à imagem é um direito autónomo com proteção constitucional, a par de outros direitos de personalidade, no n.º 1 do art.º 26º da Constituição da República Portuguesa, abrangendo, entre outros, o direito da pessoa não ser fotografada nem ver o seu retrato exposto em público sem seu consentimento.
- O retrato de uma pessoa não pode ser exposto ou publicado sem o seu consentimento
- n.º 1 do art.º 79º do C. Civil.
- O carácter inalienável e irrenunciável dos direitos de personalidade não impede, de facto, a sua limitação através do consentimento do lesado, admitindo-se, no artigo 81.º do CC, com carácter geral, a limitação voluntária dos direitos de personalidade.
- Podem, assim, as pessoas renunciar ou restringir os seus direitos de personalidade por via do consentimento, ficando com isso impedidas de invocar, depois, a ilicitude das lesões respetivas, numa espécie de concretização do brocardo '*volenti non fit injuria*'.
- Dispõe o art.º 28.º, n.º 1 da Lei n.º 58/2019, de 8 de agosto (Lei da Proteção de Dados Pessoais), que "o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo".

#### 4. Comentário

Do Douo Acórdão resulta que o direito à imagem, consubstanciado por exemplo no retrato de uma pessoa, é um direito de personalidade, com carácter inalienável e irrenunciável, podendo, contudo, o seu titular renunciar ou restringir esse seu direito por via do consentimento.

Na verdade, para que se verifique a validade do consentimento na captação, reprodução ou publicação da sua própria imagem não se torna imprescindível que a manifestação da vontade do titular do direito à imagem se submeta a uma determinada formalidade ou formalmente preconcebida, bastando, para tal, somente, que a conduta do titular do direito se torne compatível com essa captação da sua imagem.

Ora, no caso em apreço, afigura-se que, tendo o titular do direito à imagem (o trabalhador) dado o seu consentimento verbal para a captação e publicação da sua imagem pela empresa (empregador), de forma livre, específica e informada, estava a empresa autorizada a utilizá-la, quer na revista publicitária, quer no seu website. Tendo sido o consentimento considerado validamente prestado, tal não pode configurar uma violação do direito à imagem do trabalhador.

O Acórdão justifica a validade do consentimento prestado com base no preceituado na alínea g) do art.º 4.º do Regulamento Geral sobre a Proteção de Dados (RGPD), fundamentando: *No caso que nos ocupa o Autor (trabalhador), conforme resulta dos factos apurados, deu o seu consentimento verbal para a captação e publicação da sua imagem pela Ré (entidade empregadora). Este consentimento mostra-se válido porquanto foi prestado na sequência de solicitação para a publicação de tal fotografia na revista publicitária da Ré e no seu website, o que o Autor compreendeu e assentiu, permitindo-nos assim a conclusão que o mesmo corresponde a uma manifestação de vontade, livre, específica e informada como consta da definição do art.º 4º, g) do Regulamento (UE) 679/2016, de 27 de Abril) [...].*

Acrescenta ainda o Douo Acórdão que: ... a “manifestação de vontade, livre, específica e informada” que corresponde à definição de consentimento contida na al. h) do art.º 3º da Lei 67/98, de 26/10 (em vigor à data dos factos, apesar de entretanto ter sido revogada pela Lei 58/2019, de 8/8, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 679/2016, de 27 de Abril, o que para o caso concreto se revela indiferente, dado o seu carácter inovatório e não interpretativo) não corresponde, como pretendem os AA., a uma “autorização expressa, específica e escrita” (ou seja, à “manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco,

que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”, segundo a nova definição constante do art.º 4º do referido Regulamento (UE) 679/2016, de 27 de Abril).

Importa aqui, realçar o preceituado no n.º 1 do art.º 7.º do RGPD que impende sobre o responsável pelo tratamento de dados pessoais a obrigatoriedade de demonstrar que o titular dos dados deu o seu consentimento, sendo que “sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados.<sup>207</sup>”

Deste modo, verifica-se que o Regulamento deixa aos responsáveis pelo tratamento de dados pessoais a liberdade para desenvolver procedimentos que visem o cumprimento da demonstração da obtenção do consentimento; porém, para o cabal cumprimento desta obrigação do responsável pelo tratamento, não devem ser solicitados excessivos dados para tratamento adicional, *i.e.*, apenas devem ser recolhidos os dados suficientes para mostrar a validade para o tratamento (mostrar que foi obtido consentimento), sendo que não devem ser recolhidas mais informações do que as necessárias aos fins a que se destinam.

Porém, após terminar a atividade de tratamento, a prova do consentimento não deve ser conservada mais do que o necessário para o cumprimento de um dever legal ou para efeitos de declaração, exercício ou defesa de direitos num processo judicial<sup>208</sup>.

Questão diferente em análise, corresponde ao pedido de devolução de todas as cópias dos documentos pessoais entregues pelo trabalhador aquando da celebração do contrato de trabalho, incluindo o cartão de cidadão, carta de condução, cartão europeu de saúde, entre outros, deve o mesmo improceder, já que a lei prevê, expressamente, que o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais.

Anote-se a existência de limites definidos quer no Código do Trabalho, quer em legislação complementar, que legitima a continuação do tratamento de dados pessoais mesmo após a cessação do vínculo laboral, desde logo:

---

<sup>207</sup> Nos termos do considerando 42) do RGPD *ab initio*.

<sup>208</sup> Em conformidade com as alíneas b) e e) do n.º 3 do art.º 17.º do RGPD – (...) b) *Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; e, e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.*

- O n.º 1 do art.º 337.º do Código do Trabalho – permite à entidade patronal guardar, pelo **período de um ano**, contado a partir do dia da cessação do contrato de trabalho (prazo de prescrição e prova do crédito de empregador ou de trabalhador emergente de contrato de trabalho, da sua violação ou da sua cessação), os dados necessários para efeitos de gestão pessoal e administrativa;

- O n.º 4 do art.º 202.º do Código do Trabalho – impõe à entidade patronal o arquivo pelo **período de cinco anos**, das cópias dos documentos relativos ao trabalhador, “para efeitos de contratualização e execução dos seguros obrigatórios de acidentes de trabalho<sup>209</sup>.”

- O n.º 1 do art.º 19.º do Decreto-Lei n.º 28/2019, de 15 de fevereiro – impõe à entidade patronal o arquivo e a conservação pelo **prazo de dez anos** de todos os livros, registos e respetivos documentos, para efeitos de cálculo e processamento de retribuições.

Como nota final, realçamos que, o Douo Acórdão não se pronuncia sobre uma questão que excede as relações laborais entre empregador e trabalhador – a fotocópia do cartão de cidadão da esposa -, efetivamente, *o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais, se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador, nos termos da alínea a) do n.º 3 do art.º 28.º da Lei n.º 58/2019, de 8 de agosto<sup>210</sup>.*

---

<sup>209</sup> Uma vez que é de cinco anos o prazo de prescrição do direito ao pagamento por parte do segurador ao abrigo do preceituado no n.º 2 do art.121.º do Decreto-Lei n.º 72/2008, de 16 de Abril, do mesmo modo que nos termos do n.º 5 do art.º 73-B da Lei n.º 102/2009, de 10 de setembro, o cumprimento das obrigações referentes à promoção da segurança e saúde no trabalho o empregador deve manter a documentação relativa à realização das atividades a que se referem os números anteriores à disposição das entidades com competência inspetiva durante cinco anos.

<sup>210</sup> Salientamos que a alínea a) do n.º 3 do artigo 28º da Lei n.º 58/2019, de 8 de agosto, é desaplicada pela CNPD conforme Deliberação/2019/494 e com a seguinte fundamentação:

*Dispõe o n.º 3 do artigo 28.º que «salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; (...).»*

*A Alínea 11) do artigo 4.º do RGPD exige que o consentimento, para ser juridicamente relevante e, assim, corresponder ao fundamento de licitude do tratamento de dados, tem de ser livre, pelo que só quando estejam verificadas condições que garantam a liberdade de manifestação de vontade do titular é que esta pode ser considerada. Sendo certo que, como é conhecido no considerando 43 do RGPD, «[...] em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, o consentimento não deve ser tido como fundamento válido de licitude deste».*

*Não obstante admitir-se a natureza não paritária da relação laboral, decorre do princípio da dignidade da pessoa humana a necessidade de reconhecer ao indivíduo, mesmo no contexto de relações jurídicas em que, por regra, ele carece de proteção em relação à outra parte, o mínimo de livre arbítrio para gozar do seu direito fundamental à autodeterminação informacional – portanto, na dimensão jus-fundamental de controlo dos dados que lhe digam respeito –, reconhecido no artigo 35.º da CRP e no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.*

*É nesta mesma linha, que o Grupo de Trabalho do Art. 29.º (GT29) e o Comité Europeu de Proteção de Dados têm entendido, embora recusando por regra relevância jurídica ao consentimento dos trabalhadores, que estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas.*

*Ora, o disposto na alínea a) do n.º 3 do artigo 28.º, ao determinar precisamente a solução oposta, restringe excessivamente a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio dos trabalhadores mesmo quando há condições para a sua manifestação sem risco para os seus*

Ainda que o fornecimento ao empregador da fotocópia do cartão de cidadão da esposa do trabalhador, tivesse como âmbito uma vantagem jurídica ou económica para o trabalhador, uma vez terminado o vínculo laboral, cessou a legitimidade para o tratamento deste dado pessoal, além de que é um dado pessoal relativo a terceiro.

---

*direitos e interesses. Nessa medida, esta disposição traduz uma restrição injustificada e desproporcionada do disposto na alínea a) do n.º 1 do artigo 6.º e da alínea a) do n.º 2 do artigo 9.º do RGPD. Entende, assim, a CNPD que esta disposição não corresponde a uma medida legislativa nacional adequada que salvaguarde a dignidade, os direitos fundamentais e os interesses legítimos do trabalhador, não cumprindo, portanto, os requisitos exigidos na alínea b) do n.º 2 do artigo 9.º e do n.º 2 do artigo 88.º do RGPD. Em suma, por traduzir uma restrição não adequada, desnecessária e excessiva do direito fundamental à autodeterminação informacional ou à proteção dos dados enquanto direito ao controlo dos seus próprios dados, para lá do que é necessário à salvaguarda dos direitos e interesses dos trabalhadores, a alínea a) do n.º 3 do artigo 28.º da Lei n.º 58/2019 restringe o âmbito de aplicação da alínea a) do n.º 1 do artigo 6.º e da alínea a) do n.º 2 do artigo 9.º do RGPD. Com esse fundamento, a CNPD, de forma a assegurar a plena efetividade do RGPD, desaplicará a referida normas nas situações que venha a apreciar.*



## **Acórdão do Tribunal da Relação de Coimbra**

**Processo: 302/19.2T8MGL.C1**

**Relator: Sílvia Pires**

**Descritores: proteção de dados, direito à imagem, consentimento do interessado**

**Data do Acórdão: 29.06.2021**

**Legislação nacional: artigos 26.º, n.º 1 da CRP; 79.º, n.º 1 e 81.º do Código Civil; artigo 4.º, g) do Regulamento (EU) 679/2016, de 27 de abril e alínea h) do artigo 3.º da Lei n.º 67/98, de 26 de outubro (lei revogada em junho de 2019, mas em vigor à data dos factos); Lei n.º 58/2019, de 8 de agosto.**

### SUMÁRIO

I – O direito à imagem é um direito autónomo com proteção constitucional, a par de outros direitos de personalidade, no n.º 1 do art.º 26º da Constituição da República Portuguesa, abrangendo, entre outros, o direito da pessoa não ser fotografada nem ver o seu retrato exposto em público sem seu consentimento.

II - O retrato de uma pessoa não pode ser exposto ou publicado sem o seu consentimento - n.º 1 do art.º 79º do C. Civil.

III - O carácter inalienável e irrenunciável dos direitos de personalidade não impede, de facto, a sua limitação através do consentimento do lesado, admitindo-se, no artigo 81.º do CC, com carácter geral, a limitação voluntária dos direitos de personalidade.

IV - Podem, assim, as pessoas renunciar ou restringir os seus direitos de personalidade por via do consentimento, ficando com isso impedidas de invocar, depois, a ilicitude das lesões respetivas, numa espécie de concretização do brocardo 'volenti non fit injuria'.

V - Dispõe o art.28.º, n.º 1 da Lei n.º 58/2019, de 8 de Agosto (Lei da Proteção de Dados Pessoais), que *"o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo"*.

### DECISÃO TEXTO INTEGRAL

#### **Acordam na 3ª secção cível do Tribunal da Relação de Coimbra**

O Autor intentou a presente ação contra a Ré, pedindo que na procedência da ação seja:

- Julgada definitivamente ilegal e abusiva e violadora de direitos a utilização da imagem do Autor por parte da Ré;
- Julgado que tal utilização constitui uma lesão grave e dificilmente reparável à manutenção do direito de personalidade, imagem e reserva da intimidade da vida privada do Autor.
- Deve a Ré ser condenada a remover e a destruir os folhetos publicitários/revistas publicitárias "... de 02 de janeiro de 2019, assim como a remover, do seu website, a fotografia do Autor e todas e quaisquer referências a ele respeitantes.
- Condenada a Ré a não utilizar a imagem do Autor para fins publicitários ou outros de cariz comercial, por qualquer meio, sem a sua obtenção prévia, específica, negociada e acordada de autorização.

- Deve a Ré, ainda, ser condenada a proceder à entrega de todas as cópias de documentos (cópia do cartão de cidadão, carta de condução, cartão de qualificação de motorista, cartão de condutor (tacógrafo) cartão europeu de saúde, fotografia tipo passe, boletim de vacinas, fotocópia de cartão de cidadão da esposa), que se encontram na sua posse, bem como abster-se de os difundir, divulgar ou publicitar por qualquer forma.

- Deve, também, a Ré ser condenada a pagar ao aqui Autor a quantia de 24.000,00 € (vinte e quatro mil euros), a título de indemnização por danos não patrimoniais, acrescida de juros à taxa legal de 4% desde a sua citação e até integral pagamento.

Para fundamentar as suas pretensões o Autor alegou, conforme consta do relatório da sentença que de seguida se reproduz: '... trabalhou para a ré entre os dias 4 de Dezembro de 2018 e 22 de Fevereiro de 2019, data em que acordaram o termo do contrato de trabalho e que no início do mês de Fevereiro de 2019 teve conhecimento de que uma fotografia sua, captada durante o período de formação que efectuou na ré, havia sido colocada numa revista publicitária, designada "...", pertencente à ré, com uma tiragem ali indicada de 500 exemplares, a qual foi captada, impressa e publicada naquela revista publicitária sem o conhecimento e consentimento expresso do autor, facto de que a ré tinha plena consciência.

Adiantou o autor que até ao dia de hoje aludida revista publicitária permanece em circulação, facto que exterioriza a vontade da ré em fazer perdurar no tempo a divulgação da fotografia do autor, e que dias mais tarde verificou que a mesma fotografia havia sido também afixada no website «www...com/pt/...» e permanece, desde inícios de Fevereiro de 2019 até à data da instauração da acção acessível a qualquer internauta que consulte o referido website, no qual a fotografia foi publicada, novamente, à revelia do autor, sem o seu conhecimento e consentimento expresso.

Mais refere o autor que a ré é um dos maiores grupos ibéricos de transportes, oferecendo serviços de transporte, distribuição e logística em todo o território europeu, tendo, por isso, uma ampla e vasta networking com os mais diversos clientes, razão pela qual a divulgação da imagem do autor, através dos mencionados website e revista publicitária, não se circunscreve apenas ao território português, atravessando fronteiras, impossibilitando o autor de travar ou sequer controlar a aludida divulgação, o que acarreta consequências irreversíveis que jamais poderão ser integralmente reparadas. Por outra parte, menciona o autor que sempre se pautou por ser uma pessoa muito reservada e discreta, sendo avesso a redes sociais, não tendo, por conseguinte, conta no facebook, instagram, twitter ou qualquer outro website, pois que nunca teve intenção de expor a sua vida nem a sua imagem em qualquer plataforma on-line, acrescentando que é oriundo de famílias de elevado prestígio e consideração no distrito de ..., sendo, inclusivamente, familiar próximo de um ..., sem que, contudo, tenha alguma vez querido obter, com os seus laços familiares, qualquer espécie de relevância mediática.

Afirma o autor que a ré tem conhecimento da origem familiar do autor, pretendendo através da associação da sua imagem à família do autor desenvolver o seu mercado de negócios no distrito de ..., criar uma ligação ainda mais próxima com a cidade e expandir, desta forma, a sua carteira de clientes, sendo que dessa forma o autor vê afectados, ilícita e culposamente, os seus direitos à imagem e à reserva da intimidade da vida privada, o que lhe causou um profundo mau estar e perturbação, sentindo-se vexado, desrespeitado e desconsiderado na sua honra, tanto mais que a ré pretende, unicamente, locupletar-se à sua custa, sendo que depois do termo do vínculo laboral que os uniu jamais pretendeu estar associado à ré.

Acrescenta o autor que em face da utilização da sua imagem por parte da ré tem receio que outros elementos de carácter pessoal por si fornecidos à ré aquando da celebração do contrato de trabalho possam vir a ser por esta também divulgados e difundidos, tanto mais que aquando da celebração do contrato de trabalho a ré ficou

na sua posse com cópias de vários documentos, designadamente do cartão de cidadão, da carta de condução, do cartão de qualificação de motorista, do cartão de condutor (tacógrafo), do cartão europeu de saúde, da fotografia tipo passe e do boletim de vacinas do autor e de fotocópia do cartão de cidadão da sua esposa, devendo ser a ré condenada a devolver-lhe tais cópias de tal documentação, bem como a não mais utilizar, difundir ou divulgar, qualquer um daqueles documentos, assim como quaisquer outros que tenha em seu poder.'.

A Ré contestou, concluindo pela improcedência da ação e pela condenação do autor como litigante de má-fé em multa e em indemnização a seu favor, nos termos que constam do relatório da sentença que continuamos a transcrever: '... como o autor bem sabe, no final do mês de Janeiro de 2019 a ré realizou nas suas instalações uma reportagem fotográfica com o intuito de ilustrar a revista "...", a qual tem como objetivo divulgar aos seus leitores notícias de relevo e com interesse para o sector dos transportes de mercadorias, bem como as iniciativas e projetos a que a ré se vai dedicando em prol da melhoria do serviço prestado e das condições de trabalho dos seus motoristas, publicação essa sem periodicidade regular e que tem um carácter meramente informativo, e não comercial, sem qualquer cariz publicitário, sendo apenas distribuída internamente na empresa e cujo público alvo são os motoristas da ré.

Adianta a ré que para ilustrar a notícia dos bons resultados obtidos com a iniciativa ecodriva adoptada pela empresa, escolheu e publicou em tal revista a fotografia que, durante a supra referida reportagem, havia captado do autor e do colega ..., captação e publicação essas que, como o autor não ignora, fez com o conhecimento e consentimento prévio do autor, tanto mais que no momento que antecedeu a captação da imagem foi transmitido ao autor que as fotografias tiradas seriam publicadas na revista denominada "...", e no site da empresa, tendo o autor compreendido, aceite e consentido em tais factos, mostrando-se, até, encantado com a publicação da sua fotografia.

Nesse sentido, menciona a ré que os direitos à imagem e à reserva da intimidade da vida privada do autor não foram, por qualquer forma, afectados. Acrescenta a ré que não auferiu, nem auferiu, com a referida publicação qualquer proveito económico, nem pretendeu associar a imagem do autor à família deste, designadamente com o intuito de com isso obter algum benefício financeiro, tanto mais que da referida publicação nem sequer consta identificado o nome do autor por forma a que a associação do mesmo a um qualquer seu familiar de prestígio, cuja identidade e relação de parentesco a ré desconhece, sem obrigação de conhecer, pudesse suscitar-se.

Afirma a ré que não lhe é exigível qualquer indemnização, sendo que ao captar e publicar a fotografia em apreço, com o prévio consentimento do autor para o efeito, atuou em total respeito pelo disposto no art.79.º do Código Civil e no Regulamento Geral sobre a Protecção de Dados, sendo que nunca, até à data da instauração dos presentes autos, o autor transmitiu à ré o seu descontentamento ou a sua alegada falta de consentimento para a captação e publicação da imagem dos autos.

Já no que concerne à demais documentação referida pelo autor diz a ré que mesma lhe foi entregue pelo autor, que autorizou a respetiva reprodução, no âmbito da relação laboral que os uniu para efeitos, nomeadamente, e para além do mais, do seu recrutamento, execução do seu contrato de trabalho, incluindo o cumprimento das obrigações legalmente previstas na lei e nas convenções coletivas e na gestão, planeamento e organização do trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos da cessação da relação de trabalho, documentos que a ré está legitimada e obrigada por lei a guardar e tratar sem o consentimento do autor e dentro dos limites impostos pelo Regulamento Geral sobre a

Protecção de Dados, ainda não tendo decorrido o prazo legalmente estabelecido para a ré manter os documentos em questão na sua posse.'.

Notificado da contestação apresentada pela ré, o autor juntou o requerimento de fls.55 a 60, pronunciando-se no sentido da improcedência do pedido formulado pela ré no sentido da sua condenação como litigante de má-fé.

Mais requereu o autor que seja a ré condenada como litigante de má-fé, pois que com o documento que juntou com a contestação pretende alterar conscientemente a verdade, inventando uma suposta autorização e consentimento do autor para captação e divulgação da sua fotografia, sendo que da análise do próprio documento em questão se extrai que tal conclusão que a ré pretende retirar não corresponde à verdade. Veio a ser proferida sentença que julgou a causa nos seguintes termos:

Em face de tudo o exposto

Julgo a presente ação parcialmente procedente e, em consequência:

- a) condeno a ré a, no futuro, não utilizar a imagem do autor e os documentos mencionados em rr) dos factos provados para fins publicitários ou outros de cariz comercial, por qualquer meio, sem obtenção prévia, específica, negociada e acordada de autorização do autor;
- b) absolvo a ré de todos restantes pedidos contra si formulados pelo autor. Condeno o autor como litigante de má-fé em multa que fixo em 3Ucs e no pagamento da indemnização à ré consubstancia no reembolso das despesas que a mesma suportou nos presentes autos com os honorários dos seus mandatários, em montante liquidar após junção aos autos dos elementos referentes às despesas suportadas pela ré a esse título, os quais a ré deverá juntar no prazo de 10 dias. Absolvo a ré do pedido da sua condenação como litigante de má-fé formulado pelo autor.

O Autor interpôs recurso, formulando as seguintes conclusões:

...

A Ré apresentou resposta, pugnado pela confirmação da sentença.

#### **1. Do objecto do recurso**

Considerando que o objecto do recurso é delimitado pelas conclusões formuladas, as questões a apreciar são as seguintes:

- Nulidade da sentença
- Impugnação da matéria de facto
- Do consentimento do Autor para a publicação da sua imagem
- Do pedido de condenação da Ré na entrega de todas as cópias de documentos do Autor e da sua mulher
- Da litigância de má-fé.

## 2. Nulidade da sentença

O Autor imputa à sentença proferida o vício da nulidade consistente no excesso de pronúncia no concernente à sua condenação como litigante de má-fé na indemnização a favor da Ré no montante de €2.700,00.

O art.º 608º, n.º 2, do C. P. Civil, determina que o juiz deve resolver todas as questões que as partes tenham submetido à sua apreciação, exceptuadas aquelas cuja decisão esteja prejudicada pela solução dada a outras. Não pode ocupar-se senão das questões suscitadas pelas partes, salvo se a lei lhe permitir ou impuser o conhecimento oficioso de outras.

A nulidade prevista na alínea d) do n.º 1 do artigo 615º do C. P. C. – *quando o Juiz deixe de pronunciar-se sobre questões que devesse apreciar ou conheça de questões de que não podia tomar conhecimento* – verifica-se quando o Juiz deixe de tomar posição sobre todas as causas de pedir invocadas na petição, sobre todos os pedidos formulados e mesmo sobre as exceções suscitadas ou de conhecimento oficioso, isto sem prejuízo do conhecimento de alguma delas prejudicar a apreciação das restantes – artigo 660º, n.º 2, do C. P. C.

Da conjugação das normas citadas o juiz deve pronunciar-se sobre todas as questões que sejam submetidas à sua apreciação, mas está, naturalmente, impedido de se pronunciar sobre questões não submetidas ao seu conhecimento: no primeiro caso – se não se pronunciar sobre todas as questões – existirá uma omissão de pronúncia, no segundo caso – conhecer de questões não submetidas à sua apreciação – ocorrerá um excesso de pronúncia.

Os fundamentos invocados como integrantes da aludida decisão não colhem, pois, o excesso de pronúncia, antes integrando o mérito da decisão o qual consubstanciará um erro de julgamento.

Deste modo não se verifica a aludida nulidade por excesso de pronúncia.

## 3. Os factos

O Autor, revelando a sua discordância sobre o julgamento da matéria de facto, pretende, nos pontos que identifica, que a mesma após reapreciação dos meios de prova que julga pertinentes seja modificada no sentido que propõe. Os pontos em causa são os provados sob as alíneas l) , m), w) e os não provados sob os n.º 1 e 2, cuja redacção é a seguinte:

l) Mais tendo solicitado ao autor autorização para a publicação de tal fotografia na revista publicitária da ré e no seu website;

m) Tendo o autor, que compreendeu o que foi solicitado, consentido na captação e publicação mencionadas em k) e l);

ww) Após a cessação do contrato de trabalho referido em d) e e) o autor fez diligências tendentes a obter da ré um montante superior àquele que recebeu na ocasião mencionada em j).

Não provados:

1. A fotografia referida em n) e o) foi captada, impressa e publicada na revista mencionada em p) e no sítio da internet identificado em r) sem o conhecimento e o consentimento expresso do autor;

2. Facto que era do conhecimento da ré.

Assim, são os seguintes os factos provados:

a) A autora é uma sociedade comercial anónima que, há mais de 50 anos, se dedica, além do mais, à atividade de transportes;

b) Desenvolvendo tal atividade em toda a europa, com delegações em quatro países;

c) Sendo um dos maiores grupos ibéricos de transportes, oferecendo serviços de transporte, distribuição e logística em todo o território europeu, tendo, por isso, uma ampla e vasta networking com os mais diversos clientes;

d) No dia 4 de Dezembro de 2018 o autor e a ré celebraram, sob a forma verbal, um contrato de trabalho entre si;

e) No âmbito do qual o autor se obrigou a desempenhar as funções de motorista de viaturas pesadas de âmbito nacional e internacional;

f) O autor iniciou as funções referidas em e) no dia 7 de Dezembro de 2018;

g) Tendo permanecido em formação até ao dia 27 de Janeiro de 2019;

h) No dia 22 de Fevereiro de 2019 o autor e a ré acordaram o termo do vínculo laboral referido em d) e e);

i) O que ocorreu por iniciativa da ré, que afirmou ao autor pretender cessar tal vínculo, denunciando o contrato de trabalho no período experimental;

j) Tendo nessa ocasião o autor e a ré acordado entre si o montante a pagar pela ré ao autor como decorrência da cessão do vínculo laboral, o qual foi pago pela ré ao autor;

k) Em data não concretamente apurada, mas no final do mês de Janeiro de 2019 e durante o período de formação referido em g), ..., trabalhadora da ré, responsável pelo departamento de marketing, solicitou ao autor e a ..., responsável pela formação de motoristas da ré, a captação de uma fotografia;

l) Mais tendo solicitado ao autor autorização para a publicação de tal fotografia na revista publicitária da ré e no seu website;

m) Tendo o autor, que compreendeu o que foi solicitado, consentido verbalmente na captação e publicação mencionadas em k) e l);

n) Na sequência do aludido em k) a m), ... captou a fotografia retratada a fls. 36 dos autos;

o) Na qual o autor surge ao volante de um veículo da ré, tendo ao seu lado ...;

p) A qual foi publicada pela ré na revista denominada "... " referente ao mês de Janeiro de 2019, num artigo denominado "P... reconhece melhores eco motoristas pelo 3.º ano consecutivo", visando ilustrar os resultados obtidos com a iniciativa eco drive adoptada pela ré;

- q) Não constando de tal artigo o nome do autor;
- r) E no site denominado www...com;
- s) Com a ligação “www....”;
- t) A revista mencionada em p) é publicada com uma periodicidade irregular;
- u) Tendo a revista referente ao mês de Janeiro de 2019, que não foi retirada de circulação, tido uma tiragem de quinhentos exemplares;
- v) A revista mencionada em p) tem um carácter unicamente informativo e publicitário dos seus conteúdos;
- w) Não tendo carácter comercial;
- x) A revista mencionada em p) é distribuída apenas, de forma gratuita, nas instalações da ré;
- y) Tendo como público alvo os motoristas da ré;
- z) E tendo como objetivo divulgar aos seus leitores notícias de relevo e com interesse para o sector dos transportes de mercadorias, bem como as iniciativas e projectos a que a ré se vai dedicando em prol da melhoria dos serviços prestados e das condições de trabalho dos seus motoristas;
- aa) Tendo a ré utilizado a fotografia referida em n) e o) para ilustrar a notícia dos bons resultados obtidos com a iniciativa denominada eco drive por si adoptada;
- bb) Ao publicar a fotografia referida em n) e o) na revista e no sítio da internet mencionados em p) e r) a ré não pretendeu associar a imagem do autor à sua família;
- cc) Desconhecendo a ré na data da publicação da fotografia referida em n) e o) na revista e no sítio da internet mencionados em p) e r) as relações familiares do autor;
- dd) Não sendo a publicação da fotografia referida em n) e o) acompanhada do nome do autor;
- ee) Em data não concretamente apurada, mas no início do mês de Fevereiro de 2019, o autor teve conhecimento da publicação da fotografia referida em n) e o) na revista mencionada em p);
- ff) E em data também não concretamente apurada, mas no início do mês de Março de 2019, o autor teve conhecimento da publicação de tal fotografia no sítio na internet referido em r);
- gg) Em data não concretamente apurada, mas depois de ter sido citada nos presentes autos, a ré retirou a fotografia mencionada em n) e o) do seu site referido em r);
- hh) O autor é uma pessoa reservada e discreta;
- ii) Não sendo utilizador de redes sociais, não tendo conta no facebook, no twitter ou em qualquer outro website;
- jj) Nunca tendo querido expor a sua vida, nem a sua imagem, para além do mencionado em m), em qualquer plataforma online;



- kk) O autor é oriundo de famílias de elevado prestígio e consideração no distrito de ...;
- ll) Sendo sobrinho de um ...;
- mm) Nunca tendo o autor querido obter qualquer relevância mediática através dos seus laços familiares;
- nn) A ré não auferiu, nem auferiu, qualquer proveito económico com a publicação da fotografia referida em n) e o) nos termos relatados em p) e r);
- oo) Nem pretendeu associar a imagem do autor à família deste com o intuito de obter um benefício financeiro;
- pp) Nunca, até à data da instauração dos presentes autos, o autor transmitiu à ré a sua insatisfação decorrente da captação e da publicação da fotografia referida em n) e o) nos termos relatados em p) e r);
- qq) Nem até essa ocasião alegou perante a ré falta de consentimento para a captação e publicação de tal fotografia;
- rr) Aquando da celebração do contrato referido em d) e e) o autor entregou à ré fotocópia do seu cartão de cidadão, da sua carta de condução, do seu cartão de qualificação de motorista, do seu cartão de condutor, do seu cartão europeu de saúde, do seu boletim de vacinas, de uma fotografia tipo passe a si respeitante e do cartão de cidadão da sua esposa;
- ss) Autorizando a ré a reproduzir os mesmos para efeito de preenchimento/inscrição do ficheiro individual de funcionário, necessários e inerentes ao contrato de trabalho mencionado em d) e e);
- tt) Destinando-se os documentos referidos em rr) a instruir o contrato de trabalho do autor e ao cumprimento por parte da ré de obrigações previstas na lei e em convenções colectivas de trabalho;
- uu) Mantendo a ré em seu poder os documentos mencionados em rr) e tratando-os dentro dos limites impostos pelo Regulamento Geral Sobre a Protecção de Dados;
- vv) O que faz para efeitos de gestão pessoal e administrativa, de manutenção obrigatória de registo dos tempos de trabalho, de contratualização e execução de seguros obrigatórios de acidentes de trabalho, de cumprimento das obrigações referentes à promoção da segurança e saúde no trabalho e de cálculo e processamento de retribuições;
- ww) Após a cessação do contrato de trabalho referido em d) e e) o autor fez diligências tendentes a obter da ré um montante superior àquele que recebeu na ocasião mencionada em j).

## 1. O direito aplicável

### 1.1 Do consentimento do Autor para a publicação da sua imagem

O Autor coloca em crise o entendimento seguido na decisão recorrida quanto à validade do seu consentimento enquanto auto limitativo do seu direito à imagem, invocando nomeadamente que o mesmo não está suportado por qualquer documento.

O direito à imagem é um direito autónomo com protecção constitucional, a par de outros direitos de personalidade, no n.º 1 do art.º 26º da Constituição da República Portuguesa, abrangendo, entre outros, o direito da pessoa não ser fotografada nem ver o seu retrato exposto em público sem seu consentimento.

O retrato de uma pessoa não pode ser exposto ou publicado sem o seu consentimento - n.º 1 do art.º 79º do C. Civil

*O carácter inalienável e irrenunciável dos direitos de personalidade não impede, de facto, a sua limitação através do consentimento do lesado, admitindo-se, no artigo 81.º do CC, com carácter geral, a limitação voluntária dos direitos de personalidade. Podem, assim, as pessoas renunciar ou restringir os seus direitos de personalidade por via do consentimento, ficando com isso impedidas de invocar, depois, a ilicitude das lesões respectivas, numa espécie de concretização do brocardo volenti non fit injuria. III*

No acórdão de 7.6.2011 do S. T. J.<sup>121</sup>, citado na decisão recorrida, consta, relativamente ao consentimento como forma de autolimitação do direito à imagem: *A lei permite – cfr. artigo 79.º do Código Civil - que a indisponibilidade do direito à própria imagem seja excepcionada se o titular do direito der o seu consentimento na captação, reprodução e publicitação da sua imagem. Exige-se que o consentimento seja “expresso” “o que constitui uma garantia de que, efectivamente, o titular está de acordo com a intromissão de um terceiro num bem da personalidade do próprio”. Não é, no entanto, exigível que o consentimento assuma uma forma solene ou formal, mas tão só que ele seja dessumível ou inferível de “facta concludência”. Vale por dizer que para que alguém conceda o consentimento na captação, reprodução ou publicação da sua própria imagem não se torna imprescindível que o manifesto da sua vontade se submeta a uma forma predeterminada ou formalmente preconcebida, bastando, tão só, que a conduta atuada pelo titular do direito se torne compatível com a mencionada captação de imagem.*

No caso que nos ocupa o Autor, conforme resulta dos factos apurados, deu o seu consentimento verbal para a captação e publicação da sua imagem pela Ré. Este consentimento mostra-se válido porquanto foi prestado na sequencia de solicitação para a publicação de tal fotografia na revista publicitária da Ré e no seu website, o que o Autor compreendeu e assentiu, permitindo-nos assim a conclusão que o mesmo corresponde a uma *manifestação de vontade, livre, específica e informada* como consta da definição do art.º 4º, g) do Regulamento (UE) 679/2016, de 27 de Abril) e na al. h) do art.º 3º da Lei 67/98, de 26/10 – lei revogada em Junho de 2019, mas em vigor à data dos factos.

*... a “manifestação de vontade, livre, específica e informada” que corresponde à definição de consentimento contida na al. h) do art.º 3º da Lei 67/98, de 26/10 (em vigor à data dos factos, apesar de entretanto ter sido revogada pela Lei 58/2019, de 8/8, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 679/2016, de 27 de Abril, o que para o caso concreto se revela indiferente, dado o seu carácter inovatório e não interpretativo) não corresponde, como pretendem os AA., a uma “autorização expressa, específica e escrita” (ou seja, à “manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito*

sejam objeto de tratamento”, segundo a nova definição constante do art.º 4º do referido Regulamento (UE) 679/2016, de 27 de Abril).<sup>131</sup>

Importa, pois, julgar acertada a decisão recorrida quanto à validade do consentimento do Autor para a divulgação da sua foto no site da Ré e na sua newsletter.

## **2. Do pedido de condenação da Ré na entrega de todas as cópias de documentos do Autor**

O Autor discorda da decisão recorrida na parte em que julgou improcedente o seu pedido de condenação da Ré a entregar-lhe todas as cópias do seu cartão de cidadão, da sua carta de condução, do seu cartão de qualificação de motorista, do seu cartão de condutor, do seu cartão europeu de saúde, do seu boletim de vacinas, de uma fotografia tipo passe a si respeitante e do cartão de cidadão da sua esposa, que alega ter-lhe entregue aquando da celebração do contrato de trabalho que os uniu.

Quanto a este aspeto subscrevemos inteiramente o que consta da decisão recorrida: ‘Ora, a tal propósito resultou provado que aquando da celebração do contrato de trabalho que os uniu o autor entregou à ré fotocópia dos supra aludidos documentos, destinando-se os mesmos a instruir o contrato de trabalho do autor e a dar cumprimento a obrigações previstas na lei e em convenções colectivas de trabalho que incumbem à ré.

Por outra parte, ficou demonstrado que a ré mantém em seu poder tais documentos, tratando-os dentro dos limites impostos pelo Regulamento Geral Sobre a Proteção de Dados, o que faz para efeitos de gestão pessoal e administrativa, de manutenção obrigatória de registo dos tempos de trabalho, de contratualização e execução de seguros obrigatórios de acidentes de trabalho, de cumprimento das obrigações referentes à promoção da segurança e saúde no trabalho e de cálculo e processamento de retribuições (v. alíneas uu) e vv) dos factos provados).

4.2. A este propósito diga-se que a conduta da ré não merece censura, antes se encontrando legalmente suportada e legitimada.

Com efeito, dispõe o art.28.º, n.º 1 da Lei n.º 58/2019, de 8 de Agosto (Lei da Proteção de Dados Pessoais), que “o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo”.

E o certo é que, desde logo, impõe-se à ré, enquanto entidade patronal que foi do autor, guardar, pelo período de um ano, os dados necessários para efeitos de gestão pessoal e administrativa, na medida em que nos termos do preceituado no art. 337.º, n.º 1 do Código do Trabalho é de um ano, contado a partir do dia da cessação do contrato de trabalho, o prazo de prescrição do crédito de empregador ou de trabalhador emergente de contrato de trabalho, da sua violação ou da sua cessação.

Por outra parte, ainda como decorrência de tal qualidade, impõe-se à ré a guarda de tais elementos pelo prazo de cinco anos para efeitos de manutenção obrigatória do registo dos tempos de trabalho, nos termos do preceituado no art. 202.º, n.º 4 do Código do Trabalho, para efeitos de contratualização e execução dos seguros obrigatórios de acidentes de trabalho, pois que é de cinco anos o prazo de prescrição do direito ao pagamento por parte do segurador ao abrigo do preceituado no art.121.º, n.º 2 do D.L. n.º 72/2008, de 16 de Abril, e para efeitos de cumprimento das obrigações decorrentes da Lei n.º 102/2009, de 10 de Setembro, referente à promoção da segurança e saúde no trabalho, pois que, nos termos do seu art.73.º-B, n.º 5 o empregador deve manter a

documentação relativa à realização das atividades a que se referem os números anteriores à disposição das entidades com competência inspetiva durante cinco anos. Acresce que deve ainda a ré guardar tais elementos durante o período de 10 anos para os dados necessários para efeitos de cálculo e processamento de retribuições, sendo que de acordo com o art.19.º, n.º 1 do D.L. n.º 28/2019, de 15 de Fevereiro, os sujeitos passivos são obrigados a arquivar e conservar em boa ordem todos os livros, registos e respetivos documentos de suporte pelo prazo de 10 anos.

É certo que a ré deve tratar todos os supra referidos elementos dentro dos limites impostos pelo Regulamento Geral Sobre a Proteção de Dados e em respeito do mesmo, sendo certo que não resultou demonstrado, nem o autor o alegou, que no tratamento dos documentos que o autor pretende que lhe sejam devolvidos a ré desrespeite o legalmente consagrado a propósito da proteção de dados, procedendo apenas a pretensão do autor no sentido de que a ré não utilize os documentos em questão para fins diferentes dos supra mencionados, designadamente que os difunda, divulgue ou publicite para fins publicitários ou de cariz comercial sem prévia autorização do autor. 4.3. Finalmente diga-se que sempre caberia à esposa do autor, caso o pretendesse, exigir a ré a entrega da cópia do seu cartão de cidadão, o que não fez.

Encontra-se assim justificada a improcedência desta pretensão, não colidindo, a conduta da Ré, com o princípio da minimização de dados segundo o qual os dados a tratar devem ser adequados, pertinentes e limitados ao que é exigido pelas finalidades que determinam o tratamento.

## **1.2 Da condenação do Autor como litigante de má-fé**

O Autor foi condenado como litigante de má-fé em multa no montante de 3 UC e em indemnização de €2.700,00, valor do qual discorda com fundamento que esse valor foi aquele que o mandatário da Ré apresentou após a prolação da sentença, mas antes de fixado o referido valor.

Contra tal condenação o Autor esgrime dois argumentos: esse valor corresponde a despesas futuras que não se encontram justificadas e não foi reclamado pela Ré. Quanto ao primeiro deles reproduzimos integralmente o que a esse respeito consta da decisão por ter a nossa concordância:

*'Na sentença datada de 12/11/2020, exarada a fls.89 a 137, além do mais, foi o autor condenado como litigante de má-fé em multa fixada em 3Ucs e no pagamento da indemnização à ré consubstancia no reembolso das despesas que a mesma suportou nos presentes autos com os honorários dos seus mandatários, tendo sido determinada a notificação da ré para juntar elementos referentes às despesas suportadas a tal respeito por forma a liquidar-se o montante da condenação.*

*Na sequência de tal notificação a ré informou ter despendido o montante de €2.700,00 como os honorários pagos ao seu mandatário, juntando a factura/recibo constante de fls.142, emitida em 26/11/2020, da análise da qual resulta que a ré pagou a quantia global de €2.700,01 a título de honorários, com IVA incluído, ao seu mandatário. Desde logo, refira-se que não tem qualquer sentido a afirmação do autor no sentido de que tal factura/recibo não pode ser atendida porquanto emitida 13 dias após a data da notificação da ré para juntar elementos respeitantes aos honorários por si despendidos, pois que, além do mais, não é razoável que se exigisse que o ilustre mandatário da ré emitisse tal documento na própria data da sua notificação. Por outra parte, não colhe a afirmação do autor no sentido de que é exagerado o montante peticionado pela ré referente aos honorários que afirma ter pago ao seu mandatário.*

Com efeito, para sustentar a sua posição alega o autor que não se percebe que num processo como o presente um mandatário, colocado na posição de um normal mandatário, consiga ir além de 10 horas de trabalho, tanto mais que a os autos têm uma complexidade mediana, não se justificando o montante de €100,00 como valor/hora praticado na comarca de Mangualde, pois que afirma a ré que o seu mandatário despendeu não menos de 27 horas no exercício do mandato judicial. Acrescenta o autor que apesar de a petição inicial conter 78 artigos, 47 deles são alusivos a doutrina e jurisprudência, relativamente aos quais a ré se limitou a nada dizer na contestação, para além de uma simples referência genérica e de negação vertida nos artigos 16.º e 17.º da contestação.

Ora, desde logo, cremos que o número de horas mencionado pela ré como correspondendo àquelas despendidas pelo seu mandatário no exercício do mandato judicial se afigura razoável, sendo que a pecar sempre será por defeito. Destarte, não olvida certamente o autor que a actividade de um advogado no âmbito de um processo judicial não se limita ao estudo do processo. Com efeito, existem, entre o mais, reuniões com os constituintes, a análise de documentos, o estudo das questões técnicas e jurídicas, a elaboração de peças processuais e a participação em diligências.

Veja-se a este propósito que a audiência final realizada nestes autos no dia 27 de Outubro de 2020, na qual esteve presente o ilustre mandatário da ré, decorreu entre as 10h15m e as 12h50m e entre as 14h08m e as 15h23m.

Assim, na audiência final propriamente dita esteve o mandatário da ré cerca de quatro horas, a que naturalmente acresce o tempo despendido com as deslocações. Admitindo, também por defeito, que o mandatário da ré gastou 1 hora em deslocações, sobrar-lhe-iam, na tese do autor, 5 horas.

E, ainda segundo o autor, essas 5 horas seriam suficientes para o mandatário da ré estudar e preparar o processo e elaborar a contestação, isto para não falar nas reuniões que o ilustre mandatário naturalmente manteve com a sua constituínte. Absolutamente irrazoável.

E diga-se, ainda a este respeito, que os presentes autos não revestem a reduzida complexidade que o autor agora aponta, não só pela extensão dos articulados, mas também pela especificidade da matéria em discussão, relacionada com a tutela dos direitos de personalidade, que exigem estudo.

Atentas as questões suscitadas nos autos, espelhadas na petição inicial, na contestação e nos documentos juntos, e atendendo à prática dos ilustres causídicos na área de competência deste Juízo Local e aos critérios estabelecidos no art. 105.º, n.º 3 do Estatuto da Ordem dos Advogados (Lei n.º 145/2015, de 9 de Setembro), o montante reclamado a título de honorários (€2.700,00) afigura-se-nos razoável, adequado e equilibrado. Mais se refira que não tem qualquer sentido a afirmação do autor no sentido de que não pode ser atendido o montante mencionado pela ré porquanto o mesmo não se mostra suportado por qualquer laudo de honorários.

Destarte, incumbia à ré juntar os elementos necessários à liquidação do montante por si dependido com os honorários suportados com o seu mandatário, o que fez, não se justificando a junção de qualquer laudo de honorários.

A Ré formulou pedido de condenação do Autor como litigante de má-fé em multa e indemnização a seu favor de montante correspondente aos honorários dos seus mandatários pelo que a condenação em causa está justificada. Assim, improcede este fundamento do recurso.

**Decisão:**

Nos termos expostos, confirmando-se a decisão recorrida julga-se improcedente o recurso.

Custas do recurso pelo Autor.

Coimbra, em 29/06/2021

\*\*\*

<sup>111</sup> Acórdão do S. T. J. de 3.5.2019, relatado Catarina Serra e acessível em [www.dgsi.pt](http://www.dgsi.pt) .

<sup>112</sup> Relatado por Gabriel Catarino e acessível em [www.dgsi.pt](http://www.dgsi.pt) .

<sup>113</sup> Acórdão do T. R. L. de 26.9.2019 relatado por António Moreira e acessível em [www.dgsi.pt](http://www.dgsi.pt) .



**Segundo o advogado-geral J. Richard de la Tour, os Estados-Membros podem permitir às associações de defesa dos interesses dos consumidores exercer ações coletivas contra a violação da proteção dos dados pessoais<sup>211</sup>**

*Estas ações devem basear-se na violação de direitos que o Regulamento Geral sobre a Proteção de Dados confere aos titulares dos dados*

Na Alemanha, a Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (Federação das Associações de Consumidores dos Estados Federados) acusa a Facebook Ireland de ter violado, no âmbito da disponibilização de jogos gratuitos fornecidos por terceiros <sup>212</sup>, no «App-Zentrum» («Centro de aplicações») da plataforma, regras em matéria de proteção dos dados pessoais, de combate à concorrência desleal e de proteção dos consumidores. Neste contexto, a Federação intentou nos tribunais alemães uma ação inibitória contra a Facebook Ireland.

Segundo o Bundesgerichtshof (Supremo Tribunal Federal, Alemanha), a Facebook Ireland não forneceu aos utilizadores (de forma concisa, transparente, inteligível e de fácil acesso, numa linguagem clara e simples) as informações necessárias relativas à finalidade do tratamento dos dados e ao destinatário dos dados pessoais. Assim, segundo esse tribunal, a Facebook Ireland violou o Regulamento Geral sobre a Proteção de Dados <sup>213</sup>.

Todavia, o Bundesgerichtshof tem dúvidas quanto à admissibilidade da ação intentada pela Federação.

Com efeito, interroga-se sobre a questão de saber se uma associação de defesa dos interesses dos consumidores como a Federação ainda tem, depois da entrada em vigor do Regulamento Geral sobre a Proteção de Dados, legitimidade ativa para intentar uma ação nos tribunais cíveis contra violações deste regulamento,

<sup>211</sup> Acessível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-12/cp210216pt.pdf>

<sup>212</sup> Ao consultar certos jogos no Centro de aplicações, em 26 de novembro de 2012, o utilizador podia ver um determinado número de informações premindo o botão «Sofort spielen» (Jogar agora). Resulta, em substância, dessas informações que a utilização da aplicação em causa permitia à sociedade que fornecia os jogos obter um determinado número de dados pessoais e a autorizava a proceder a publicações, em nome do utilizador, de certas informações, como a sua pontuação nos jogos. Esta utilização implicava a aceitação, por parte do utilizador, das cláusulas contratuais gerais da aplicação e da sua política em matéria de proteção de dados. Além disso, no caso do jogo «Scrabble», é indicado que a aplicação é autorizada a publicar o estado, fotos e outras informações em nome do utilizador.

<sup>213</sup> Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1). [www.curia.europa.eu](http://www.curia.europa.eu)



independentemente da violação concreta do direito de uma pessoa à proteção dos seus dados pessoais e sem um mandato conferido por essa pessoa.

Considera, nomeadamente, que se poderia deduzir do facto de o regulamento conferir às autoridades de controlo poderes alargados em matéria de supervisão, de investigação e de adoção de medidas corretivas que a fiscalização da aplicação do referido regulamento incumbe principalmente a essas autoridades.

Por conseguinte, o Bundesgerichtshof pediu ao Tribunal de Justiça que interpretasse o regulamento.

**Nas suas conclusões de hoje, o advogado-geral Jean Richard de la Tour propõe ao Tribunal de Justiça que interprete o Regulamento Geral sobre a Proteção de Dados no sentido de que não se opõe a uma regulamentação nacional que permite às associações de defesa dos interesses dos consumidores agirem judicialmente contra o presumível autor de uma violação da proteção dos dados pessoais, invocando a proibição das práticas comerciais desleais, a violação de uma lei em matéria de proteção dos consumidores ou a proibição da utilização de cláusulas contratuais gerais inválidas, desde que a ação coletiva em causa se destine a fazer respeitar os direitos que esse regulamento confere às pessoas objeto do tratamento impugnado.**

O advogado-geral recorda que, no seu Acórdão *Fashion ID*<sup>214</sup>, o Tribunal de Justiça se pronunciou sobre uma questão semelhante, a propósito da Diretiva 95/46<sup>215</sup>, que precedeu o Regulamento. O Tribunal de Justiça declarou que essa diretiva não se opõe a uma regulamentação nacional que permite às associações de defesa dos interesses dos consumidores agirem judicialmente contra o presumível autor de uma violação da proteção dos dados pessoais.

O advogado-geral considera que nem a substituição da diretiva por um regulamento nem a circunstância de o regulamento ter passado a consagrar um artigo à representação dos titulares dos dados no âmbito de ações judiciais são suscetíveis de pôr em causa o entendimento do Tribunal de Justiça naquele acórdão.

Assim, segundo ele, **os Estados-Membros ainda podem prever a possibilidade de certas entidades exercerem, sem mandato dos titulares dos dados e sem que seja necessário invocar a existência de casos concretos a propósito de pessoas individualmente designadas, ações coletivas destinadas a proteger os interesses coletivos dos consumidores, desde que seja invocada a violação de disposições deste regulamento que têm por objeto conferir direitos subjetivos aos titulares dos dados.**

**Ora, é esse efetivamente o caso da ação inibitória que foi intentada pela Federação contra a Facebook Ireland.**

O advogado-geral considera igualmente que o regulamento não se opõe a disposições nacionais que habilitam uma associação de defesa dos interesses dos consumidores a intentar uma ação inibitória com vista a garantir o respeito dos direitos por ele conferidos, por intermédio de regras que têm por objeto proteger os consumidores ou combater as práticas comerciais desleais.

Com efeito, essas regras podem conter disposições semelhantes às que constam do regulamento, em especial no que diz respeito à informação dos titulares dos dados quanto ao tratamento dos seus dados pessoais. Por conseguinte, a violação de uma regra relativa à proteção dos dados pessoais pode simultaneamente implicar a

---

<sup>214</sup> Acórdão do Tribunal de Justiça de 29 de julho de 2019, *Fashion ID* [C-40/17; v., igualmente, C n.º 99/19].

<sup>215</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31).

violação de regras relativas à proteção dos consumidores ou às práticas comerciais desleais.

**Segundo o advogado-geral, a defesa dos interesses coletivos dos consumidores por associações é especialmente adaptada ao objetivo do regulamento de estabelecer um nível elevado de proteção dos dados pessoais.**

---

**NOTA:** As conclusões do advogado-geral não vinculam o Tribunal de Justiça. A missão dos advogados-gerais consiste em propor ao Tribunal, com toda a independência, uma solução jurídica nos processos que lhes são atribuídos. Os juízes do Tribunal iniciam agora a sua deliberação no presente processo. O acórdão será proferido em data posterior.

**NOTA:** O reenvio prejudicial permite aos órgãos jurisdicionais dos Estados-Membros, no âmbito de um litígio que lhes seja submetido, interrogar o Tribunal de Justiça sobre a interpretação do direito da União ou sobre a validade de um ato da União. O Tribunal não resolve o litígio nacional. Cabe ao órgão jurisdicional nacional decidir o processo em conformidade com a decisão do Tribunal. Esta decisão vincula do mesmo modo os outros órgãos jurisdicionais nacionais aos quais seja submetido um problema semelhante.

---

*Documento não oficial, para uso exclusivo dos órgãos de informação, que não vincula o Tribunal de Justiça.*

*O [texto integral](#) das conclusões é publicado no sítio CURIA no dia da leitura.*

*Contacto Imprensa: Cristina López Roca ( (+352) 4303 3667.*

*Imagens da leitura das conclusões estão disponíveis em "[Europe by Satellite](#)" ( (+32) 2 2964106.*





IV\_Recensões



## **Teoria Geral do Direito Digital: Transformação Digital Desafios para o Direito,**

**Wolfgang Hoffmann-Riem, 2021**

*Cristina Maria de Gouveira Caldeira*

*(...) a transformação digital traz consigo oportunidades para melhorar as condições de vida, mas também riscos para o bem-estar dos indivíduos e para a preservação de uma ordem social justa."*

Wolfgang Hoffmann-Riem, 2021, p.4<sup>216</sup>

Wolfgang Hoffmann-Riem, Professor Associado de Inovação e Direito da Bucerius Law School, Hamburgo, e Professor Catedrático de Direito Público e Administração Pública na Universidade de Hamburgo, foi Juiz do Tribunal Constitucional Federal da Alemanha entre 1999 e 2008, tendo-se destacado como relator no domínio da proteção de dados.

Na obra *Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito*, o autor apresenta-nos uma visão atualizada e muito clara das principais temáticas relacionadas com o fenómeno da digitalização, explorando os desafios que a sociedade digital coloca ao Direito.

No capítulo introdutório, Wolfgang Hoffmann-Riem sublinha que no último milénio ocorreram duas inovações tecnológicas "disruptivas" sustentáveis, as quais provocaram profundas convulsões na sociedade: a impressão tipográfica e a industrialização. Porém, desde o final do milénio enfrentamos uma nova convulsão, desta vez, tecnológica, que tal como as duas anteriores provocará uma alteração profunda no tecido social. Trata-se da transformação digital da economia, da cultura, da política e da comunicação. Algoritmos, *big data*, inteligência artificial, robótica e *blockchain*, são as palavras-chaves que Wolfgang Hoffmann-Riem utiliza para caracterizar o desenvolvimento a que se assiste nestes novos tempos.

O termo "digitalização", inicialmente associada às tecnologias e às infraestruturas (*software* e *hardware*), representa hoje uma mudança fundamental nas condições de vida desencadeadas pela sua utilização em todo o mundo. A multiplicidade de novos modelos de negócio e a criação de valor alcançado, bem como o aparecimento de novas qualificações, como a engenharia de software, a segurança das tecnologias de informação, a *cloud computing* ou a *data analytics*, são os reflexos do paradigma digital.

Centrando-se no impacto da transformação digital no ordenamento jurídico, o autor reflete sobre se as regras legais tradicionais respondem aos desafios levantadas pela sociedade atual. A grande questão, reside em saber "como podem ser alcançados os objetivos de bem-estar público, para além das oportunidades para a sociedade como um todo e para os indivíduos no uso da digitalização, tendo em vista os riscos envolvidos?". Em resposta, o autor convida-nos a refletir sobre a governança

<sup>216</sup> Hoffmann-Riem, Wolfgang. *Teoria Geral do Direito Digital: Transformação Digital Desafios para o Direito*, Tradução Italo Fuhrmann, Editora Forense, Rio de Janeiro, 2021.

digital e, defende que além dos modelos tradicionais de governança, o controlo baseado em algoritmos de comportamento e estruturas “*algorithmic Regulation*” é assumidamente um novo modo de governança que pode complementar os modelos tradicionais (“*governance mix*”). Na visão do autor, importa associar a digitalização a oportunidades de inovação sustentável, facto que o legislador deverá atender, sob pena de se perder o potencial da inovação e do desenvolvimento.

Em suma, a obra centra-se nos desafios que a sociedade digital coloca ao Direito, e apresentando conceitos sólidos de natureza técnica (algoritmos, IA, *big data*, entre outros), explora a diferença entre regras legais e digitalizadas, o controle digital do comportamento, os desafios jurídicos relacionados com a proteção de dados e a proteção dos direitos fundamentais face aos desafios da digitalização.

Atento às interdependências científicas, económicas, culturais e políticas transnacionais no campo dos serviços digitais e dos modelos de negócios, o autor remete-nos para soluções jurídicas globais. E, nessa medida, a harmonização jurídica europeia em algumas áreas, designadamente na área da proteção de dados, são observadas como exemplo. No entanto, realça as diferenças que existem na abordagem jurídica dos vários países terceiros, a exemplo da China, cujos ajustes poderão ser alcançados mais rapidamente, por via das exigências que são colocadas pelas empresas que atuam globalmente.







