Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 04 – ABRIL 2022
ONLINE

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

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

Data: abril 2022
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. A Revista é dirigida por uma diretora: Cristina Maria de Gouveia Caldeira, que é co-coordenadora do Privacy and Data Protection Centre, email: centro.data-protection@universidadeeuropeia.pt

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

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

9.º Periodicidade. A Revista terá periodicidade quadrimestral.

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

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

Ficha Técnica

Título
Privacy and Data Protection Magazine

Subtítulo
Revista Científica na Área Jurídica

Número
004

Ano de Publicação
2022

Afiliação
Privacy and Data Protection Centre – Universidade Europeia

Autores
Andrei Ferreira Fredes
Cristina Maria de Gouveia Caldeira
Duilio Landell de Moura Berni
Gabrielle Bezerra Sales Sarlet
José Roberto Coldim
Márcia Santana Fernandes
Rita Girão Curro
Sylvia Chaves da Silva Ramos
Vera Lúcia Raposo

Prefácio
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

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

ISSN
2184-920X

Número de Registo
127600

Propriedade
Ensilis - Educação e Formação, Unipessoal, Lda.

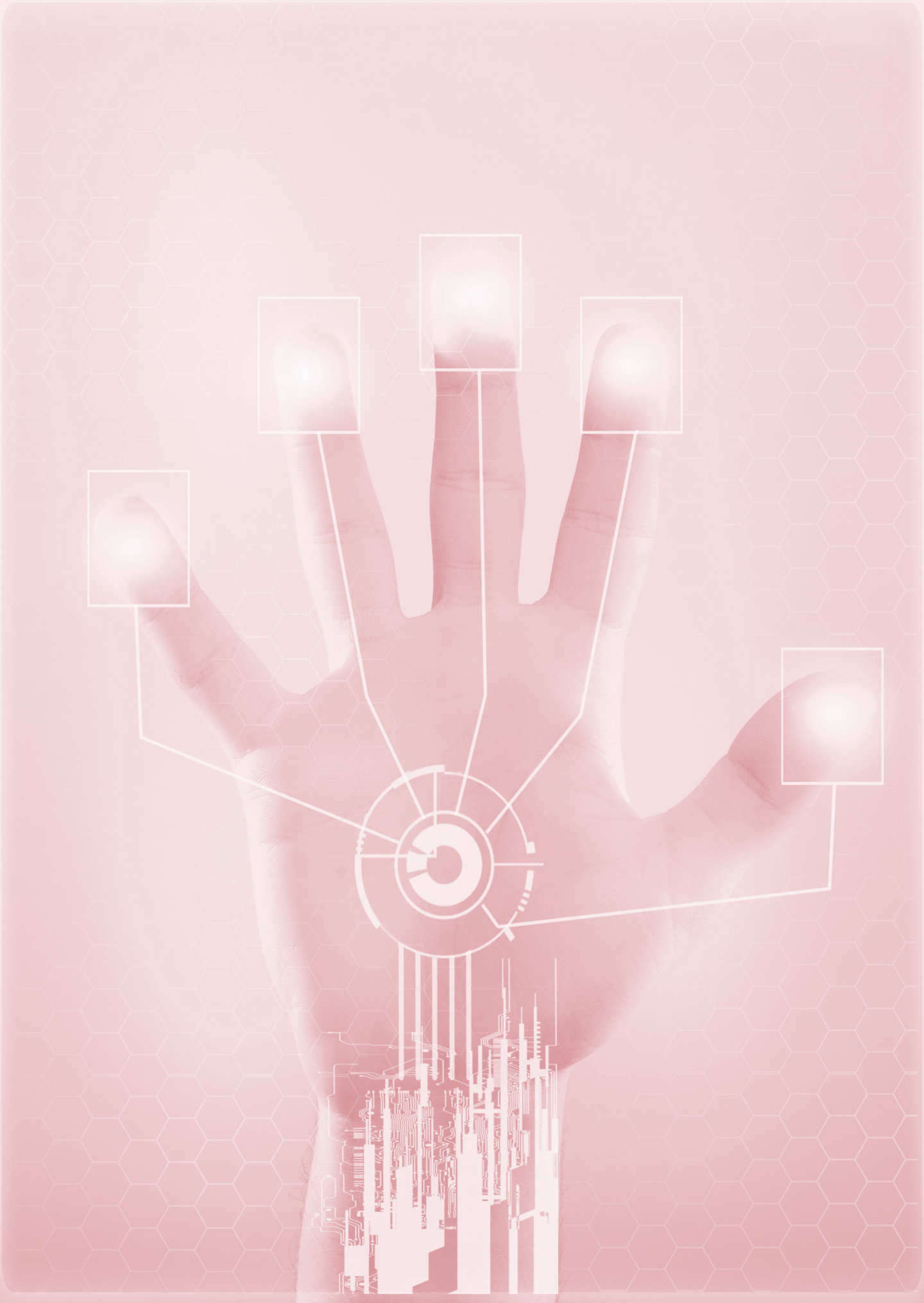
Chief Executive Officer
Miguel Carmelo

NIPC/NIF
504 669 788

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

PRIVACY AND DATA PROTECTION CENTRE

Índice



Prefácio

A revista *Privacy and Data Protection Magazine* celebra o seu primeiro ano, reafirmando o compromisso de publicar regularmente, em acesso aberto, artigos relevantes na área do Direito, contribuindo desse modo para o aprofundamento da doutrina jurídica.

Na sua parte doutrinária, a presente publicação versa, a partir de ângulos de entrada não estranhos ao seu espírito diretor, sobre temáticas centrais do ponto de vista de uma problematização do estado atual das democracias de tipo ocidental, com especial atenção ao político-constitucional no mundo de língua portuguesa: a discussão sobre a potencial caracterização dos "nossos" Estados de derivação liberal como Estados Digitais-Vigilantes; a questão da protecção das «liberdades comunicativas» em face da disseminação de desinformação nos ambientes virtuais; a (boa) reacção do dever ser jurídico aos indesejáveis usos das chamadas «*deep fakes*», concretamente.

Com relevância teorética e dogmática para uma leitura informada dos ordenamentos jurídicos atuais, discute-se ainda a questão do estatuto do Direito Digital enquanto disciplina jurídica autónoma, tendo especialmente presente o caso brasileiro.

Em sede de "outros estudos", inclui-se, também como expressão de interesse editorial pela área do direito da saúde, uma análise técnico-jurídica, no horizonte da Lei de Proteção de Dados brasileira, sobre os distintos processos de consentimento na pesquisa envolvendo seres humanos e na assistência à saúde.

A secção sobre Legislação e Jurisprudência Comentadas abre-se a um comentário ao Acórdão do Tribunal de Justiça, de 5 de abril de 2022, proferido no âmbito do Processo C-140/20, incindindo sobre a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002 [ato normativo sobre o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrónicas], lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia.

Sendo o Direito do Consumo uma área abrangida pelo objeto da revista, justifica-se outrossim a inclusão do Comunicado de Imprensa n.º 68/22 do Tribunal de Justiça (Luxemburgo, 28 de abril de 2022) sobre o Acórdão no processo C-319/20/Meta Platforms Ireland [anteriormente Facebook Ireland, responsável pelo tratamento de dados pessoais dos utilizadores da rede social em linha Facebook na União], nos termos do qual: «As associações de defesa dos consumidores podem intentar ações coletivas contra violações da proteção dos dados pessoais. Esse tipo de ações pode ser intentado independentemente da violação concreta do direito à proteção dos dados de um titular e sem mandato desse titular para o efeito».

Por último, apresenta-se, em sintonia com as preocupações presentes na parte doutrinária da publicação, a recensão da atualíssima obra de Byung-Chul Han, *Não-Coisas, Transformações no Mundo em que Vivemos*. Tradução Ana Falcão Bastos, Editora Relógio D´Água Editores, Janeiro de 2022.

Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

I_Artigos Doutrinários

You Can Run, But You Can't Hide – Digital State's Surveillance in Liberal Democracies[1]

Vera Lúcia Raposo [2]

RESUMO

O estado digital é um estado de vigilância. A necessidade de atingir propósitos relevantes para o Estado (incluindo a segurança pública) e a disponibilidade de avançadas ferramentas digitais, incentivam o Estado a controlar os movimentos de seus cidadãos, inclusive nas democracias liberais. A vigilância do Estado não é necessariamente ilegal. O critério decisivo para avaliar a legitimidade das práticas de vigilância reside nos objetivos a serem alcançados e nos direitos legais garantidos aos seus cidadãos.

PALAVRAS-CHAVE

Vigilância do Estado; ferramentas digitais; democracias liberais; privacidade; Proteção de dados

[1] The author wishes to thank the editorial team of The Digital Constitutionalist (https://digi-con.org/), where this text was initially published (on the 23 de March 2022, at https://digi-con.org/you-can-run-but-you-cant-hide/), and that so kindly authorised this republication.

[2] Professora na Faculdade de Direito da Universidade de Coimbra, vera@fd.uc.pt

You Can Run, But You Can't Hide – Digital State's Surveillance in Liberal Democracies

Vera Lúcia Raposo

ABSTRACT

The digital State is a surveillance State. The need to reach relevant State purposes (including public safety) and the availability of developed digital tools, encourage the State to control the movements of its citizens, including in liberal democracies. State's surveillance is not necessarily unlawful. The ultimate criteria to assess the legitimacy of surveillance practices lies in the objectives to be achieved and in the legal rights guaranteed to its citizens.

KEYWORDS:

State's surveillance; digital tools; liberal democracies; privacy; data protection

Introduction

The digital world! As exciting as it can be, it is also an enormous Big Brother, where the State (and also private entities) can know, at any given moment, everything you do. The State is a classic vigilant of our actions, but now, with the digital world, it has gained substantial opportunities for the surveillance of communications, movements, political activities and all types of behaviours and affiliations of its citizens.

1. State surveillance in liberal democracies

The 'Surveillance State' has for long been acknowledged in the context of oppressive regimes, with China leading the way.[3] However, citizen mass surveillance is not restricted to authoritarian regimes. Liberal democracies also have their say on the matter. Are we being watched right now? Most likely… yes.

Whistle-blowers like Edward Snowden[4] showed the world that liberal democracies also resort to citizen surveillance. It is estimated that at least 75 countries (from a universe of 176) are using different types of AI surveillance.[5] This fact is not, per se, a sure indication that Governments are abusing the system. It all depends on the specific purpose of surveillance and on the mechanisms in place to guarantee the rules of good governance.

a) Good governance in State surveillance

The concept of good governance refers to the lawful use of power in the management of public affairs[6]. In the era of digital technologies, this concept interrelates with that of digital governance.[7] Good governance covers the respects by several different fundamental rights: privacy rights, data protection rights, freedom of expression rights, self-determination rights. Just a few words about the first two.

---

[3] Feldstein, Steven, How Much Is China Driving the Spread of AI Surveillance?, In The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace, 2019.

[4] Snowden, Edward. Permanent Record. Picado Paper, 2019.

[5] NOURI, Steve, How AI Is Making an Impact on the Surveillance World, Forbes, 4 December 2020, https://www.forbes.com/sites/forbestechcouncil/2020/12/04/how-ai-is-making-an-impact-on-the-surveillance-world/?sh=9dd8dd8265ef.

[6] COUNCIL OF EUROPE, 12 Principles of Good Governance, nd, https://www.coe.int/en/web/good-governance/12-principles.

[7] OPEN GOVERNMENT PARTHERSHIP, Actions for Transparent and Accountable Digital Governance, nd, https://www.opengovpartnership.org/actions-for-transparent-and-accountable-digital-governance/.

i. Privacy rights

Traditional privacy rights - as established in Article 8 of the European Convention of Human Rights (ECHR)8 and in Article 7 of the Charter of Fundamental Rights of the European Union9 - are an obvious limit to State's intervention. In Liberty and Others v. the United Kingdom[10] the European Court of Human Rights (ECtHR) considered that the interception of telephone, facsimile, e-mail and data communications by the British Ministry of Defence was a violation of article 8 of the ECHR. More recently, in Big Brother Watch and Others v. the United Kingdom,[11] the ECtHR found again that the United Kingdom was in violation of the referred Article 8 due to its programmes of surveillance and intelligence sharing between the US and the United Kingdom. Even more recently, in Ekimdzhiev and Others v. Bulgaria,[12] the fact that the communications of anyone in the country could be intercepted and accessed by authorities was considered a violation of privacy rights. Several other cases are still pending, as for instance the case of the Association Confraternelle de la Presse Judiciaire v. France et 11 Autres Requêtes,[13] involving the French Intelligence Act of 24 July 2015.

As for Article 7 of the of the European Charter of Fundamental Rights, some of the most famous statements in its regards were made in the case of Maximillian Schrems v. Data Protection Commissioner (C-362/14).[14] Very emphatically, the Advocate General Bot wrote on its opinion: 'Such mass, indiscriminate surveillance [the Advocate General was referring to the access of the United States intelligence services to the transferred data] is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the Charter' (par. 200).[15]

---

8 Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950, https://www.echr.coe.int/documents/convention_eng.pdf.

9 Charter Of Fundamental Rights of the European Union, 2012/C 326/02, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=cs.

10 Liberty & Other Organisations v. the United Kingdom, application no. 58243/00, 1 July 2008, https://hudoc.echr.coe.int/eng#{%22appno%22:[%2258243/00%22],%22itemid%22:[%22001-87207%22]}.

11 Big Brother Watch and Others v. The United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, https://hudoc.echr.coe.int/eng#{%22appno%22:[%2258170/13%22],%22itemid%22:[%22001-210077%22]}.

12 Ekimdzhiev and Others v. Bulgaria, Application no. 70078/12, 11 January 2022, https://hudoc.echr.coe.int/fre-press#{%22itemid%22:[%22003-7224338-9824769%22]}.

13 Association Confraternelle de la Presse Judiciaire v. France et 11 Autres Requêtes, Application no. 49526/15, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-173634%22]}.

14 Maximillian Schrems v. Data Protection Commissioner, C362/14, ECLI:EU:C:2015:627, 6 October 2015, https://curia.europa.eu/juris/document/document.jsf;jsessionid=DF65240F9C4C81AF31AA31E2D3CC502B?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2927716

15 Maximillian Schrems v. Data Protection Commissioner, C362/14, ECLI:EU:C:2015:627, Opinion of Advocate General Bot, delivered on 23 September 2015, https://curia.europa.eu/juris/document/document.jsf;jsessionid=F9904F9DB366E5353741DD13DFB08FDA?text=&docid=168421&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3380194.

ii. Data protection rights

Within the European Union, data protection rights find their natural field of action in the General Data Protection Regulation (GDPR),[16] the most stringent law on data protection worldwide. If, in turn, surveillance operates in the framework of law enforcement, the applicable legal regime will be the Law Enforcement Directive (LED).[17]

Under the GDPR data processing can only take place if one of the legal grounds described in Article 6(1) fits the particular situation (the GDPR imposes several other requirements besides the demand of a legal ground, but for our current discussion this is the most relevant one). Moreover, as digital surveillance deals with sensitive data[18] (location data, biometric data), Article 9(2) also applies. Therefore, two legal grounds are required. In theory, both articles can easily provide legal grounds for State surveillance: 'performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (Article 6(1)(e) of the GDPR) and 'for reasons of substantial public interest' (Article 9(2)(g) of the GDPR).[19] In the end, it all depends on the concrete assessment made in the specific case.

The LED is structured in a different way. Data processing is considered lawful, not in face of particular scenarios, but when performed by specific authorities/bodies/entities: the ones entrusted with 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Articles 2(1) and 3(7) of the LED). Chapter II establishes the requirements to be complied with, and Article 10(1) stands out because of the special demanding regime it sets forth for sensitive data: when there is a legal base on an EU law or in national law, vital interests on the data subject or any other natural person are safeguarded, and the processing only involves data 'manifestly made public by the data subject'. This latter requirement raises the so-called 'function creep' problem', which happens when a technology created for a given aim changes its purposes, i.e., people might be willing to publicly disclose their data on social media, but not to provide those data to State's purposes.

---

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[17] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680.

[18] BLIIM, Steven, What Is Sensitive Data? Sensitive Data Definition & Types, 6 August 2020, https://www.cpprotect.com/blog/what-is-sensitive-data/

[19] INFORMATION COMMISSIONER'S OFFICE, Public Task, nd, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

b) In defence of State mass surveillance?

Surveillance can serve legitimate purposes.[20] Under this assumption, unsuspected authors – that is, not related to repressive legal regimes – have advocated State surveillance, even mass surveillance.

Crime reduction and fair justice are certainly compelling reasons to advocate in its favour. In his study 'In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance',[21] James Stacey Taylor made one of the most drastic vindications of State surveillance: 'The state should place all of its citizens under surveillance at all times and in all places, including their offices, classrooms, shops – and even their bedrooms.' In this paper Taylor highlighted the several benefits of State's mass surveillance: in court, witnesses (or any other type of evidence for that matter) would no longer be necessary because the State would know everything, which, in turn, will make it possible to guarantee a fair judicial outcome for everyone, disregarding if they are rich or poor and how talented are their lawyers. Moreover, if the State can see everything, crime would diminish due to the deterrence effect of constant surveillance.

The fight (and the protection) against terrorism is another seductive reason to advocate for State's surveillance. Under the threat of catastrophic terrorist attacks with biological or nuclear material, Persson and Savulescu advocated in favour of mass surveillance in their book Unfit for the Future.[22]

If things are put in such dramatic terms, it is very likely that many of us approve some restrictions to our privacy rights in favour of more surveillance. The question remains, though, in the precise definition of the requirements and red lines: i) when exactly can the State make use of mass surveillance? ii) when that scenario takes place, which rules/requirements should apply?

2. Tools for States' surveillance

Several top of the art digital tools – frequently provided by private companies - allow States to carry out their surveillance tasks.

Social media intelligence (SOCMINT) allows constant monitoring of online activities and the detection of potential 'risks' (mostly criminal acts) beforehand.[23] Even though social media are in the public eye (still, with different privacy settings), the fact that someone (the State) 'stalks' every tweet and every post raises privacy concerns. Adding another

---

[20] KÖNIGS, Peter, Introduction to the Special Issue on the Ethics of State Mass Surveillance, Moral Philosophy and Politics, 7(1), 2020, pp. 1-8, https://doi.org/10.1515/mopp-2020-0008.

[21] TAYLOR, James Stacey, **In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance,** Public Affairs Quarterly, 19(3), 2005, pp. 227–246, http://www.jstor.org/stable/40441413.

[22] PERSSON, Ingmar, and SAVULESCU, Julian, **Unfit for the Future: The Need for Moral Enhancement**, Oxford University Press,1st edition, 2012.

[23] PRIVACY INTERNATIONAL, Social media Intelligence, 23 October 2017,https://privacyinternational.org/explainer/55/social-media-intelligence.

layer of troubledness to this equation is the fact that such information can be used to create databases, where all the data about an individual are stored and combined, thus creating a digital profile of every citizen.[24]

Mobile telephones have been for long a source of information about the holder's location, though cell towers are not very accurate in this regard. Smartphones were a game changer. Smartphones applications (apps) can nowadays be used for everything, from paying transportation to interact with governmental bodies, thus providing very detailed information about the person. Moreover, smartphones came equipped with the Global Positioning Systems (GPS), which can collect location data[25] and thus reveal the person exact location at any given time. This, in turn, can unveil the person's religion (is the person near a mosque or a synagogue?), political affiliation (has the person attended a political rally? From a left wing or a right-wing party?) and even private sins (did a married men entered a gay bar?).

Biometric recognition[26] is also a handy tool for citizen surveillance. This wide concept includes iris recognition,[27] fingerprint identification,[28] and several other forms of identification/recognition using biometric data. Currently, facial recognition technology[29] is one of the most widely used, especially because of its convenience, as it does not require any collaboration from the person. The proliferation of facial recognition cameras makes it possible to 'check' every face passing by any public space. Facial data are analysed and transformed into a biometric template, which is then compared against a database of templates to reach an identification. The internet in general, and social media in particular, became a fruitful source of pictures (to be transformed into templates) of properly identified citizens, making it very easy to create databases with millions of templates (the collection of pictures from the internet became also a profitable business, as attested by the rise of Clearview Analytics,[30] a company whose business is to create massive databases of biometric templates with pictures collected online and then sell them to police forces worldwide).

---

[24] BRINGAS COLMENAREJO, Alejandra, The Tense Relationship Between Social Media Intelligence and Privacy, 24 October 2019, https://thesecuritydistillery.org/all-articles/the-tense-relationship-between-social-media-intelligence-and-privacy.

[25] BOSHELL, Paige M., The Power of Place: Geolocation Tracking and Privacy, 25 March 2019, https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/.

[26] SNIJDER, Max, Biometrics, Surveillance and Privacy, 2016, ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructure, https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf

[27] ELECTRONIC FRONTIER FOUNDATION, Iris Recognition, nd, https://www.eff.org/pages/iris-recognition, https://www.eff.org/pages/iris-recognition

[28] FINN, Jonathan, Photographing Fingerprints: Data Collection and State Surveillance, Surveillance and Society, 3(1), 2005, https://doi.org/10.24908/ss.v3i1.3318.

[29] Electronic Identification, Face Recognition: how it works and its safety, 15 October 2021, https://www.electronicid.eu/en/blog/post/face-recognition/en.

[30] COBLE, Sarah, Clearview AI to be Fined $22.6m for Breaching UK, Info Security Magazine, 30 November 2021, https://www.infosecurity-magazine.com/news/clearview-ico-data-fine/.

a) Are liberal democracies becoming less liberal?

Liberal democracies are becoming less liberal.[31] The rise of mass surveillance might be one of the reasons (among others) for this 'deliberalization'. Recent events – terrorism attacks, right wing extremist and the proliferation of Nazi groups, the (very real) possibility of a III World War – pressured Governments to know more about what is happening in their territories. In a sense, liberal democracies were forced to become less liberal to survive as such. This is certainly a compelling reason to accept 'some' State's surveillance. The exact quantity (How much surveillance?) and quality (When? How? Who?) is the one-million-dollar answer. Without a proper answer, liberal democracies might simply disappear. It won't be the first time that laudable purposes (the preservation of liberal democracies) lead to tragic outcomes (the very extinction of liberal democracies).

[31] OBSERVER RESEARCH FOUNDATION, Liberal Democracies Are Becoming Less Liberal Worldwide, 22 August 2018, https://www.orfonline.org/research/43509-liberal-democracies-are-becoming-less-liberal-worldwide/.

O dever constitucional de proteção das liberdades comunicativas frente à desinformação nos ambientes virtuais

Andrei Ferreira Fredes [32]
Gabrielle Bezerra Sales Sarlet [33]

RESUMO

Este ensaio tem como objetivo abordar dois pontos centrais da proteção das liberdades comunicativas no direito brasileiro. Em primeiro lugar, coloca-se o argumento que, em função especialmente de seu duplo caráter enquanto direito fundamental de dimensão subjetiva e objetiva, a liberdade de manifestação do pensamento e o direito à informação não podem restar desprotegidos frente aos avanços dos interesses econômicos das companhias tecnológicas que controlam os espaços virtuais de comunicação. Em segundo lugar, busca-se verificar quais as medidas já estabelecidas pela regulação brasileira, a fim de verificar se se apresentam como adequadas e suficientes. Conclui-se que, apesar da legislação eleitoral brasileira dar importante passo inicial, ainda há necessidade de o poder legislativo assumir sua função como protetor das garantias fundamentais e aprofundar os mecanismos de salvaguarda das liberdades comunicativas nos espaços virtuais.

PALAVRAS-CHAVE

Liberdade de Expressão, Desinformação, Direito à Informação, Direitos Fundamentais.

[32] Doutor em Direito em regime de cotutela internacional pela Pontifícia Universidade Católica do Rio Grande do Sul (Brasil) e a Universidad de Granada (España). fredesandrei@gmail.com

[33] Gabrielle Bezerra Sales Sarlet é Advogada, Mestre em direito pela UFC. Doutora em direito pela UNIA- Universidade de Augsburg(alemanha). Pos-doutoramento em Direito pela Universidade de Hamburgo(Alemanha) e pela PUCRS. Professora dos cursos de graduacao, de mestrado e de doutorado Pontifícia Universidade Católica do Rio Grande do Sul-PUCRS. Especialista em neurociencias e ciencias do comportamento PUCRS.

The constitutional duty to protect communicative freedoms in the face of disinformation in virtual environments

Andrei Ferreira Fredes
Gabrielle Bezerra Sales Sarlet

ABSTRACT

This essay aims to address two central points of the protection of communicative freedoms in Brazilian law. First, the argument is made that, especially due to its dual character as a fundamental right of subjective and objective dimension, the freedom to speech and the right to information cannot remain unprotected in the face of advances in the economic interests of technological companies that control virtual spaces of communication. Secondly, it seeks to verify which measures are already established by the Brazilian regulation, in order to verify whether they are adequate and sufficient. It is concluded that, although brazilian electoral legislation takes an important initial step, there is still a need for the legislative power to assume its function as a protector of fundamental guarantees and to deepen the mechanisms for safeguarding communicative freedoms in virtual spaces.

KEYWORDS

Freedom of Speech, Disinformation, Right to Information, Fundamental Rights.

Notas introdutórias

O Constitucionalismo foi confrontado com inúmeras crises nas duas primeiras décadas do século XXI. Inicialmente as crises econômicas, desencadeadas pela ruptura do modelo financeiro liberal e desregulamentado norte-americano, seguidas por diversos momentos de crise humanitária, com os influxos de refugiados forçados a abandonar seus países que se encontravam em conflitos armados.

Mais recentemente, restou abalado em razão da crise provocada pelo impacto dos mecanismos tecnológicos, especialmente os de comunicação digital, que se mostraram capazes de erodir a estrutura dos Estados Democráticos ao atingir diretamente o esteio da ideia de representação deliberativa sobre a qual a Democracia se sustenta[34]. Assim, como define Clara Keller, a desinformação se entende como a difusão intencional de informações falsas a fim de obter lucro, causar danos, ou avançar objetivos políticos ou ideológicos, tendo sido exponencialmente ampliada com a utilização das plataformas digitais sociais[35].

O desafio enfrentado pelas democracias pluralistas passou, de fato, a ser o equacionamento que envolve a imposição dos valores e dos princípios constitucionais, bem como a cartela de direitos e garantias fundamentais, em face das ondas antidemocráticas desencadeadas pelos sistemas organizados de desinformação nos ambientes virtuais. Contudo, em outro giro, atento à garantia da ampla liberdade comunicativa dos cidadãos usuários das redes, tendo em vista a fundamentalidade das liberdades de expressão e de informação, tanto em sua dimensão subjetiva quanto objetiva, pedra de toque da própria democracia[36]. Ou seja, a questão é buscar mecanismos apropriados para, simultaneamente, coibir os avanços das campanhas de desinformação ao tempo em que devem manter e promover a liberdade legítima de manifestação do pensamento e de difusão de informação nas mídias sociais, caracterizando-se como algo bastante complexo.

Evidentemente não se faz possível em breves páginas desenvolver esta temática por completo, o recorte que aqui se oferece é uma análise acerca de alguns mecanismos que já foram adotados no cenário brasileiro no enfrentamento da matéria. Alerta-se, antecipadamente, que a maioria deles tangenciam a legislação eleitoral, parametrizando as campanhas eleitorais, sobretudo no que toca às eleições do ano em curso, às exigências de um pleito livre e justo em conformidade com os artigos 1º, parágrafo único e artigo 14º da Constituição Federal de 1988(doravante CF/88).

Nesta medida, entende-se que se mostram como um ponto de partida importante, mas ainda insuficiente, no combate aos sistemas preordenados de desinformação orientados para as mídias sociais digitais. Alerta-se para o longo itinerário em que cabe ao

---

[34] BALAGUER CALLEJÓN, Francisco. As Duas Grandes Crises do Constitucionalismo Diante da Globalização no Século XXI. In: **Joaçaba**. v. 19, n. 3, set./dez. 2018.

[35] KELLER, Clara Iglesias. Don't Shoot the Message: Regulating Desinformation Beyond Content. In: **Revista de Direito Público**. Brasília, v. 18, n. 99, jul./set. 2021.

[36] SARLET, Ingo Wolfgang; HARTMANN, Ivar Alberto Martins. Direitos Fundamentais e Direito Privado: a Proteção da Liberdade de Expressão nas Mídias Sociais. In: **RDU**. Vol. 16. N. 90. Nov-dez 2019. Porto Alegre. 2019.

Estado atuar, em especial mediante instrumentos regulatórios, a fim de cumprir seu dever constitucional de proteção, de respeito e de promoção dos direitos fundamentais, mediante a ação dos três poderes harmonicamente ordenados, preferencialmente por intermédio do poder legislativo, o qual deve arcar com o ônus/dever de regulamentar a CF/88.

1 - O dever de proteção das liberdades fundamentais comunicativas na Constituição Federal brasileira de 1988

É possível estabelecer que, em regra, a jurisprudência e a doutrina tradicionalmente definiram o conteúdo do direito à liberdade de expressão e do direito à informação como típicos direitos de defesa. Vedada qualquer possibilidade de censura, definida a posição preferencial *prima facie* frente a outros direitos fundamentais que limitam a liberdade de expressão e, especialmente em relação ao direito à informação e de liberdade jornalística, revelou-se incompatível com a norma constitucional a limitação à veiculação apenas de fatos, sendo protegidas também as manifestações de opinião e de crítica por parte da mídia[37]. Todos esses aspectos do âmbito de proteção da liberdade de expressão e do direito à informação estão intimamente ligados ao desenvolvimento e ao adensamento da democracia e do pluralismo no contexto brasileiro[38].

Com efeito, essa interpretação liberal, decorrente da concepção de matriz burguesa de Estado, somou-se à lógica de um Estado Social, responsável por não apenas por um caráter omissivo, mas por impor uma atuação positiva na realização dos direitos e das garantias. Robert Alexy, a propósito, elabora um conceito de direito a prestações em sentido amplo, no qual inclui "a proteção do cidadão contra outros cidadãos por meio de normas de direito penal, estabelecimento de normas organizacionais e procedimentais e alcança até prestações em dinheiro e outros bens"[39].

Isto é, para Alexy, o Estado não é responsável apenas por prestações específicas definidas constitucionalmente, que tipicamente se estruturam como direitos a prestações, a exemplo dos Direitos à Saúde, à Educação, à Previdência Social, dentre outros. Para o autor, há um Direito às prestações em sentido amplo, que inclui qualquer Direito Fundamental para o qual deva o Estado agir para sua concretização, seja por meio de prestações fáticas ou normativas, como a criação de normas penais ou que regulem a atividade dos atores privados[40].

Alexy argumenta que o direito às prestações decorrentes de algum direito fundamental se sustenta "na possibilidade de encontrar na Constituição uma série de pontos de apoio, formulados de forma objetiva, para uma interpretação orientada a direitos a

---

[37] SARLET, Ingo Wolfgang; SIQUEIRA, Andressa de Bittencourt. Liberdade de Expressão e Seus Limites numa Democracia: O Caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil. In: **Revista de Estudos Institucionais.** v. 6, n. 2, maio/ago. 2020.

[38] BRASIL. Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental 130.** Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605411. Acesso em: 11 de abril de 2021.

[39] ALEXY, Robert. **Teoria dos Direitos Fundamentais.** 2ª ed. Malheiros. São Paulo. 2014. p. 442.

[40] ALEXY, Robert. Ibidem.

prestações"[41]. A título de exemplo, o autor menciona a obrigação constitucional formulada pela Lei Fundamental Alemã[42] de proteção da dignidade da pessoa humana, bem como a cláusula geral do Estado Social e o enunciado geral de igualdade, que, em casos especiais, pode fundamentar direitos originários às prestações[43].

Na doutrina nacional, a necessidade de se definir prestações positivas por parte do Estado para a fruição dos Direitos Fundamentais não é nova, Gilmar Mendes referia, já em 1993, que "a garantia dos direitos fundamentais enquanto direitos de defesa contra intervenção indevida do Estado e contra medidas legais restritas dos direitos de liberdade não se afigura suficiente para assegurar o pleno exercício da liberdade"[44], sendo necessário estabelecer garantias de natureza institucional, o que implica em um dever de prestações normativas, ou seja, um dever positivo de regular, uma vez que "não apenas a existência de lei, mas também a sua falta pode revelar-se afrontosa aos direitos fundamentais"[45].

Em relação à CF/88, é possível encontrar vários pontos de apoio, indo até mesmo além dos relacionados por Alexy a partir da Lei Fundamental alemã, principalmente em relação aos Direito de livre manifestação do pensamento e informação, tendo em vista sua essencialidade para o regime democrático. No Art. 1°, encontram-se os fundamentos do Estado, sobretudo em uma constelação que centraliza a dignidade da pessoa humana – os quais se relacionam com a liberdade de expressão em sua dimensão de autonomia – e o pluralismo político. No Art. 3°, a Constituição define como objetivo da República a construção de uma sociedade livre, justa e pacífica, sendo impossível admiti-los apenas a partir da dimensão negativa dos direitos. O Art. 5°, em sua complexidade, expressa a garantia da liberdade da manifestação da expressão e assegura a todos o acesso à informação. No Art. 220, a CF/88 estabelece que a manifestação do pensamento, expressão e informação não sofrerão qualquer restrição, vedando a censura e qualquer dispositivo que constitua embaraço à plena liberdade de informação jornalística[46].

Conjugando as disposições constitucionais que estabelecem o Estado Social e Democrático de Direito, do qual decorre o rol de limites e de deveres constitucionais, há a necessidade não apenas de abstenção estatal, mas implica em evitar que agentes privados violem os direitos alheios, especialmente numa sociedade em que a concentração de poder econômico e social é massiva. Como coloca Antonio Perez Luño, o Estado So-

---

41 ALEXY, Robert. Ibidem, p. 435.

42 DEUTSCHLAND. Lei Fundamental da Alemanha. Disponível em: https://www.btg-bestellservice.de/pdf/80208000.pdf. Acesso em: 25 ago. 2021.

43 ALEXY, Robert. Ibidem.

44 MENDES, Gilmar Ferreira. A Doutrina Constitucional e o Controle de Constitucionalidade como Garantia da Cidadania. Declaração de Inconstitucionalidade sem a pronúncia de nulidade no Direito brasileiro. In: **Revista de Direito Administrativo**. Rio de Janeiro, jan./mar. 1994. p. 49.

45 MENDES, Gilmar Ferreira. Ibidem.

46 BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 1° abr. 2021.

cial significa uma superação da ideologia individualista do laissez-faire – no qual "la creciente intervención del Estado en el terreno económico y social que crea unos derechos, los quales no pueden entenderse como Staatsschranken (limites de la acción estatal), sino como Staatszwecke (fines de la acción del Estado)". No mesmo sentido, a lição de Ingo Sarlet:

> Neste contexto, impõe-se que relembremos aqui a aceitação da ideia de que ao Estado, em decorrência do dever geral de efetivação dos direitos fundamentais, incumbe zelar – **inclusive em caráter preventivo** – pela proteção dos direitos fundamentais dos indivíduos, não só contra ingerências indevidas por parte dos poderes públicos, mas **também contra agressões provindas de particulares** e até mesmo de outros Estados, dever este que, por sua vez, desemboca na obrigação de adotar medidas positivas com vista a garantir e proteger de forma efetiva a fruição dos direitos fundamentais.[47]

Toda informação tem, em si, um emolduramento da realidade. No que toca ao Estado democrático de Direito, urge ressaltar que a formatação deve expressar os pilares da liberdade, da igualdade, do pluralismo de ideias em uma conjugação que, em razão da fidúcia na ordem democrática, assegure a vida plena e digna e a paridade de armas no jogo de poder.

Sendo assim, a partir do problema colocado pela desinformação nos ambientes virtuais, verificou-se que agentes privados – companhias tecnológicas detentoras de serviços de redes sociais de grande popularidade – podem influenciar, inclusive de forma subliminar e pervasiva, seus usuários, mediante seleção de conteúdo por seus algoritmos, permitindo alcançar objetivos que atendam aos seus próprios interesses ou aos de seus anunciantes. Além disso, em função do modo como essas redes estão estruturadas, ou seja do design, agentes particulares que delas se utilizam para disseminar conteúdos falsos ou ofensivos são igualmente prestigiados, uma vez que a polarização causada por esse tipo de conteúdo é responsável pela retenção dos usuários na rede. Por fim, todo esse sistema de controle e distribuição de conteúdo e de informação se faz de forma totalmente obscura, sob o argumento da inescrutabilidade dos algoritmos[48]. Vale destacar, nessa altura, que a opacidade é frontalmente contrária ao que se entende por soberania popular.

Dessa forma, afirma-se que não há apenas uma faculdade estatal de regular a atuação das redes sociais, mas, sim, um dever, em função dos direitos de proteção das liberdades comunicativas e da democracia, os quais, como já elaborado, em sua dimensão objetiva, constituem objetivos máximos da ordem jurídica. A dinâmica de efetividade da constituição de um Estado Social e Democrático de Direito não admite que companhias privadas possam controlar, sem qualquer transparência e responsabilidade, as liberdades comunicativas ao ponto de impactar decisivamente em processos eleitorais e demais momentos cruciais da vida social, como na recente gestão da pandemia do coronavírus.

---

[47] SARLET, Ingo Wolfgang. Eficácia dos Direitos Fundamentais: uma Teoria Geral dos Direitos Fundamentais na Perspectiva Constitucional. 12ª ed. Livraria do Advogado. Porto Alegre. 2018, grifo nosso.

[48] BALAGUER CALLEJÓN, Francisco. Redes Sociais, Companhias Tecnológicas e Democracia. In: HABERLE, Peter et al. (Orgs). Direitos Fundamentais, Desenvolvimento e Crise do Constitucionalismo Multinível. Editora Fundação Fênix. Porto Alegre. 2020.

Essa constatação não significa que haja uma única medida a ser tomada, pois, em primeiro lugar, algumas possibilidades são vedadas, tendo em vista que as liberdades que se pretende fortalecer não perdem sua dimensão como direitos de defesa. Oportunamente, vale lembrar que Alexy diz que o direito a ações estatais positivas "é formado por um feixe de posições de espécies bastante distintas"[49], no qual se incluem abstenções do Estado, proteção contra intervenção de terceiros, inclusão em procedimentos relevantes e a tomada de medidas fáticas para a efetivação do direito[50]. Da mesma forma, Ingo Sarlet menciona que "importa efetivamente é levar-se em conta a circunstância de que também os direitos a prestações abrangem um feixe complexo e não necessariamente uniforme de posições jurídicas"[51], concluindo que "podem variar quanto ao seu objeto, seu destinatário e mesmo quanto à sua estrutura jurídico-positiva, com reflexos na sua eficácia e efetivação"[52].

A ideia de um feixe de posições jurídicas também pode ser encontrada no pensamento de Clémerson Cléve, ao mencionar que "o Estado não pode deixar, igualmente, de atuar para proteger os direitos fundamentais, inclusive normativamente (dever de proteção), e de implantar políticas públicas voltadas à afirmação dos direitos"[53]. Atenta-se que, na lição de Dieter Grimm, define-se que "*los derechos de libertad pueden incorporar la protección de algunos de sus presupuestos, frecuentemente de índole material, en los casos em que la libertad quedaría sin valor alguno si no extendiera a ellos*"[54]. Igualmente, Luciano Feldens reporta que "os direitos fundamentais desencadeiam 'uma ordem dirigida' ao Estado no sentido de que a este incumbe a obrigação permanente de concretização e retaliação dos direitos fundamentais"[55]. Esses entendimentos parecem se adequar ao argumento constantemente repetido de que, para a regulação dos ambientes digitais, não há uma "bala de prata", sendo necessário pensar em um complexo de mecanismos regulatórios.

Isto posto, verifica-se que os deveres de proteção exigem uma atuação positiva do Estado, uma obrigação prestacional, na defesa de um direito de liberdade – como a liberdade de expressão, o direito à informação e a plena liberdade jornalística. Como articulam Maitê Lemos e Vinícius Deprá, "a necessidade de cooperação entre os Poderes é medida indissociável para a concretização destes direitos" e isso implica que não haja uma obrigação única e específica, mas a necessidade de todos os Poderes envolvidos

---

[49] ALEXY, Robert. Teoria dos Direitos Fundamentais. 2ª ed. Malheiros. São Paulo. 2014. p. 443.

[50] ALEXY, Robert. Ibidem.

[51] SARLET, Ingo Wolfgang. Eficácia dos Direitos Fundamentais: uma Teoria Geral dos Direitos Fundamentais na Perspectiva Constitucional. 12ª ed. Livraria do Advogado. Porto Alegre. 2018.

[52] SARLET, Ingo Wolfgang. Ibidem.

[53] CLÈVE, Clèrmerson Merlin. A Eficácia dos Direitos Fundamentais Sociais. In: **Revista de Direito Constitucional e Internacional.** v. 54. 2006. p. 28.

[54] GRIMM, Dieter. **Multiculturalidad y Derechos Fundamentales Trad**: Ignacio Gutiérrez Gutiérrez. Editorial Trotta. Madrid. 2007. p. 68.

[55] FELDENS, Luciano. Direitos fundamentais e Direito Penal: garantismo, deveres de proteção, princípio da proporcionalidade, jurisprudência constitucional penal, jurisprudência dos tribunais de direitos humanos. Porto Alegre: Livraria do Advogado, 2008. p. 65.

atuarem na concretização dos direitos fundamentais em questão. Nesse sentido, é papel do Estado como um todo não apenas regular a coerção ou punição dos excessos que transbordem da liberdade legítima, e, sim, estabelecer mecanismos capazes de proporcionar, da melhor forma, a possibilidade de todos atuarem na construção social, o que invariavelmente ocorre pela comunicação livre, conforme define Ivar Hartmann: "Um Estado Democrático de Direito requer, portanto, mecanismos legais para fomentar e promover a manifestação do pensamento, e não apenas para a prevenção de sua regulamentação abusiva"[56].

Essa ação estatal, que deve partir de todos os Poderes, ao atuar sobre as liberdades comunicativas, deve ter um sentido específico, promovendo o debate público o máximo possível do ideal do livre mercado de ideias. Isso significa que o Estado não deve ser vetor imediato de valores ou de ideias, mas guardião de um espaço que, na medida dos contornos da constituição, seja capaz de promover a liberdade comunicacional de todos, entendida como a capacidade de ouvir e ser ouvido, conforme coloca Owen Fiss: "*The duty of the state is to preserve the integrity of public debate – in much the same way as a great teacher - not to indocrinate, not to advance the 'truth', but to safeguard the conditions for true and free collective self-determination*"[57].

Se as redes sociais são espaços de exercício das liberdades comunicativas – como elas mesmas se intitulam – então não podem simultaneamente ser espaços de subtração da liberdade comunicativa pelo poder econômico, além de dissimulação por algoritmos opacos que prestigiam manifestações falsas ou ofensivas para obter engajamento, banem usuários e apagam conteúdos, sem transparência ou possibilidade de obter revisão adequada das decisões. Nesse sentido, a posição, *a priori* neutra, do Estado de garantia do espaço livre de exercício das liberdades comunicativas se revela uma posição insuficiente para a promoção da igualdade material.

Se é possível verificar que as liberdades comunicativas, e mesmo os pleitos eleitorais e o manejo de políticas públicas, ficam em risco quando não há qualquer controle sobre a forma como as redes sociais atuam sobre as manifestações e informações veiculadas na rede, é imperativo que todos os Poderes atuem no sentido de garantir um espaço virtual mais democrático, dentro dos limites constitucionalmente previstos. Isso significa que é possível propor um rol de possibilidades.

A título de exemplo, poderia ser observado desde a tipificação penal de condutas vinculadas à veiculação dolosa de notícias falsas até a garantia da transparência das aplicações dos algoritmos das redes frente a uma agência reguladora capaz de auditar esses mecanismos. A seguir verifica-se quais mecanismos já foram incorporados ao ordenamento jurídico brasileiro, que ainda carece de desenvolvimento e, em especial, de aprofundamento para que se cumpra o dever estatal de proteção das liberdades comunicativas e da garantia de eleições livres e justas.

---

[56] HARTMANN, Ivar. Liberdade de Expressão e Capacidade Comunicativa: Um Novo Critério Para Resolver Conflitos entre Direitos Fundamentais Informacionais. In: **Direitos Fundamentais e Justiça. Belo Horizonte**. ano 12, n. 39, jul./dez. 2018. p. 158.

[57] FISS, Owen. Free Speech and Social Structure. In: **Iowa Law Review**. n. 71. 1986. p. 1.416.

2 - A legislação eleitoral brasileira e o combate à desinformação

É possível destacar algumas disposições da legislação eleitoral com o objetivo de coibir e punir o uso abusivo das liberdades comunicativas. O Art. 323 do Código Eleitoral brasileiro estabelece a proibição de divulgação de fatos que se sabe inverídicos, sobre candidato ou partido político, com capacidade para exercer influência sobre o eleitorado, seja na propaganda eleitoral ou durante o período de campanha[58]. Tendo sido, ainda, a menção sobre o período de campanha adicionada recentemente por nova redação dada ao dispositivo pela Lei 14.192/21, o que significa não haver mais a exigência de que a manifestação seja na propaganda eleitoral *stricto sensu*[59], passando a alcançar qualquer manifestação durante o período de campanha que preencha os demais núcleos do tipo previsto na Lei. Além disso, adicionou-se às agravantes a hipótese de aumento de pena quando o crime for cometido por meio da Internet, hipótese que não estava prevista anteriormente e já havia sido adequadamente endereçada pela doutrina[60].

Da mesma forma, na Lei das Eleições são dispostas proibições relacionadas à atuação dos partidos e dos candidatos durante o período da campanha eleitoral. Dentre as proibições, destaca-se a vedação da possibilidade de contratação de pessoas para emissão de mensagens ou comentários na Internet visando ofender a honra ou desprestigiar a personalidade de candidato, partido ou coligação (Art. 57-H, §1°) – punível com detenção de dois a quatro anos, além de multa – reservando pena menor (seis meses a um ano) às pessoas contratadas para prestarem o serviço de envio de mensagens ou comentários vedados pelo Art. 57-H §1[61]. Além da possibilidade de pedido de suspensão temporária da veiculação do conteúdo ilegal pelos candidatos, partidos ou coligações (Art. 57-I), ao que adicionam Ingo Sarlet e Andressa Siqueira, determinação que, na prática, resulta em remoção ou exclusão do conteúdo, ainda que a norma fale em suspensão temporária[62].

Apesar dessas disposições estabelecendo condutas penalmente coibidas serem necessárias e adequadas, elas não são, em verdade, possibilidades apenas avançadas na Internet; pelo contrário, conforme demonstrado, a legislação apenas recentemente veio a se atualizar para incluir a Internet dentre as agravantes dessas condutas que podem ser realizadas por meios físicos tradicionais. Essa observação se faz necessária pois,

---

[58] Art. 323. "Divulgar, na propaganda eleitoral ou durante período de campanha eleitoral, fatos que sabe inverídicos em relação a partidos ou a candidatos e capazes de exercer influência perante o eleitorado." BRASIL. **Código Eleitoral – Lei 4.737 de 15 de Julho de 1965.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm. Acesso em: 18 set. 2021.

[59] BRASIL. **Lei 14.192 de 4 de Agosto de 2021.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14192.htm. Acesso em: 20 set. 2021.

[60] SARLET, Ingo Wolfgang; SIQUEIRA, Andressa de Bittencourt. Liberdade de Expressão e Seus Limites numa Democracia: O Caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil. In: **Revista de Estudos Institucionais.** v. 6, n. 2, maio/ago. 2020.

[61] BRASIL. **Lei das Eleições – Lei 9.504 de 30 de Setembro de 1997**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 18 set. 2021.

[62] SARLET, Ingo Wolfgang; SIQUEIRA, Andressa de Bittencourt. Liberdade de Expressão e Seus Limites numa Democracia: O Caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil. In: Revista de Estudos Institucionais. v. 6, n. 2, maio/ago. 2020.

conforme apontado, o objetivo deve ser de aprofundar as possibilidades regulatórias especificamente relacionadas às situações que os meios digitais tornaram possíveis de ocorrer, o que implica discutir mecanismos regulatórios capazes de influenciar a arquitetura das redes, como coloca Ivar Hartmann – "*the role that courts must turn to: enforcing procedural rules for content moderation and reviewing the architecture and basic rules of information flows in such platforms*"[63]. Aliás, faz sentido admoestar para a falta de fronteiras sólidas que separem o mundo real do virtual na contemporaneidade.

A legislação eleitoral brasileira regula, pelo menos de forma inicial, um tópico que envolve o estabelecimento de regras procedimentais capaz de influenciar a arquitetura das redes, que é a questão relacionada à publicidade paga e o impulsionamento de conteúdo em redes sociais por candidatos, partidos e coligações. Assim, a Lei de Eleições estabelece que a propaganda eleitoral poderá se realizar pelo meio da Internet (Art. 57-B), inclusive por meio de redes sociais (Art. 57-B, IV), em seguida estabelecendo uma distinção ao mencionar que o conteúdo pode ser gerado ou editado pelos candidatos, partidos ou coligações (Art. 57-B, IV, "a") ou por qualquer pessoa natural, sendo que, neste último caso, estaria vedado o impulsionamento de conteúdos (Art. 57-B, IV, "b").

Alguns esclarecimentos são necessários: em primeiro lugar, conforme alertam Ingo Sarlet e Andressa Siqueira, uma leitura sistemática envolvendo a Lei dos Partidos Políticos (Lei 9.096/95)[64], que estabelece a possibilidade de utilização dos recursos do fundo partidário para contratação de impulsionamento de publicidade política pelos candidatos e partidos. Além disso, outras disposições da Lei de Eleições (Lei 9.504/97) regulam questões específicas relacionadas ao manejo desse mecanismo publicitário, destacando-se a vedação de impulsionamento "para alterar o teor ou a repercussão de propaganda eleitoral" (Art. 57-B §3°), a tipificação do crime de impulsionamento ou publicação de conteúdo novo no dia da eleição (Art. 39, §5°, IV) e a obrigação de identificação inequívoca dos candidatos, partidos ou coligações responsáveis pela contratação do impulsionamento lícito de conteúdo (Art. 57-C) [65].

A partir da leitura conjunta desses dispositivos, verifica-se que a intenção do legislador foi de impedir que, por meios oblíquos, tornasse possível o financiamento de campanhas políticas sem a observação dos procedimentos adequados. Observa-se que o legislador permite o uso de recursos do fundo partidário para o impulsionamento de propaganda política, mas veda que esse impulsionamento seja realizado por alguém que não seja o próprio candidato, partido ou coligação, além de exigir destes a identificação inequívoca na publicidade, que deve ser contratada diretamente com o provedor de aplicação. Isto significa dizer que, se um candidato ou partido pretende veicular qualquer tipo de publicidade em determinada plataforma ele deve contratar diretamente com aquela plataforma, não se utilizando de serviços de terceiros, e cumprindo todos os requisitos em relação à publicização das informações em relação aos gastos e ao conteúdo da publicidade eleitoral.

---

[63] HARTMANN, Ivar. A New Framework for Online Content Moderation. In: **Computer Law and Security Review.** n. 36, 2020. p. 7.

[64] BRASIL. **Lei dos Partidos Políticos – Lei 9.096 de 19 de Setembro de 1995.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9096.htm. Acesso em: 21 set. 2021.

[65] BRASIL. **Lei das Eleições – Lei 9.504 de 30 de Setembro de 1997**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 18 set. 2021.

O objetivo da vedação é, de um lado, controlar o uso dos recursos com publicidade na Internet e, em outro giro, permitir ao eleitor averiguar o conteúdo da manifestação consciente de se tratar de publicidade paga com o objetivo de favorecer determinada candidatura. Daí, a proibição de impulsionamento de propaganda eleitoral desidentificada ou por qualquer pessoa alheia ao pleito eleitoral se apresenta justificada, conforme o próprio Supremo Tribunal Federal já atestou[66], no sentido de garantir (ou pelo menos minimizar) que não haja cooptação do embate democrático pelo poder econômico.

A essas disposições se soma a proibição de "veiculação de conteúdos de cunho eleitoral mediante cadastro de usuário de aplicação de internet com a intenção de falsear identidade (Art. 57-B §2º)"[67]. Essa disposição, igualmente fundamental e adequada, complementa as disposições anteriores, uma vez que, se não se permite a contratação de terceiros para impulsionamento de conteúdos, menos ainda poderia se imaginar juridicamente tutelada a possibilidade de se criar contas falsas para artificialmente inflar campanhas e influenciar os eleitores. Entretanto, conforme referido, essas disposições proibindo a contratação de terceiros para impulsionamento de publicações e de sistemas automatizados (*bots*) ainda é inicial e insuficiente, principalmente porque o objeto da regulação é o mesmo da propaganda eleitoral.

A legislação brasileira não oferece um conceito de propaganda eleitoral, diferentemente da legislação portuguesa, por exemplo, que define como propaganda eleitoral "toda actividade que vise directamente promover candidaturas, seja actividade dos candidatos, dos subscritores das candidaturas ou de partidos políticos que apóiem as diversas candidaturas, bem como a publicação de textos ou imagens que exprimam ou reproduzam o conteúdo dessa actividade"[68]. Contudo, a jurisprudência do Tribunal Superior Eleitoral brasileiro assentou que se entende como ato de propaganda eleitoral três situações distintas, sendo "aquele que leva ao conhecimento geral, ainda que de forma dissimulada, a candidatura, mesmo que apenas postulada, a ação política que se pretenda desenvolver ou razões que induzam a concluir que o beneficiário é o mais apto ao exercício de função pública"[69].

A interpretação do que constitui propaganda eleitoral certamente demonstra as limitações da legislação estabelecida. Se o conceito de propaganda eleitoral for demasiadamente amplo, as restrições sobre a liberdade de expressão serão demasiadas, uma vez que, pela jurisprudência do Tribunal Superior Eleitoral, configuraria propaganda eleitoral manifestações que induzam ou levem a concluir que determinado candidato é o mais apto ao exercício de função pública, consequência que se obtida poderia levar a limitação de manifestações legítimas com amparo constitucional – lembrando que o STF

---

[66] SUPREMO TRIBUNAL FEDERAL. **Ação Direta de Inconstitucionalidade 4650/DF**. Relator Ministro Luiz Fux. 2015.

[67] BRASIL. **Lei das Eleições – Lei 9.504 de 30 de Setembro de 1997**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 18 set. 2021.

[68] PORTUGAL. **Decreto-Lei nº. 319-A/76**. Disponível em: https://dre.pt/home/-/dre/655916/details/maximized. Acesso em: 21 set. 2021.

[69] Tribunal Superior Eleitoral. **Recurso Especial Eleitoral 21594/RS.** Relator Ministro Luiz Carlos Madeira. 2004.

já decidiu pela ampla liberdade de crítica, inclusive no período eleitoral[70]. De outro lado, caso a interpretação sobre o que constitui propaganda eleitoral seja muito restrita, abre-se a possibilidade para violações por meio de propaganda subliminar[71] e abuso do poder econômico, uma vez que restaria difícil configurar os casos de contratação de terceiros para criação de conteúdo com finalidade propagandística na Internet.

Além disso, como já delineado, o problema dos abusos cometidos nas redes sociais, especialmente em relação à influência no processo democrático, é muito mais complexo do que as possibilidades regulatórias hoje presentes na legislação eleitoral vigente no Brasil. Conforme os últimos anos nos apresentaram, a partir da eleição norte-americana de 2016 e da eleição de Donald Trump, foi verificado o sistema de elaboração de perfilamento dos usuários (*profiling*[72]) e envio de mensagens não aparentemente relacionadas aos candidatos, muitas vezes, os envios tinham como objetivo desestimular eleitores de estados considerados chave de irem aos locais de votação[73]. À vista disso, a regulação que se busca para o mundo digital necessariamente deve interferir/articular com a estrutura e o funcionamento dessas plataformas, direcionando sua formatação. Isto, como já referido, não invalida a legislação eleitoral e a persecução penal proposta em alguns de seus dispositivos, mas exige um aprofundamento e uma ampliação em formatações que não se resumem à norma de caráter penal.

Ademais, cumpre destacar que algumas medidas vêm sendo adotadas no âmbito administrativo. A Portaria 318 do Tribunal Superior Eleitoral[74] instituiu, no final de março de 2022, a frente nacional de enfrentamento à desinformação, composta de servidores públicos e com o objetivo de realizar ações a fim de promover e reforçar a credibilidade das instituições democráticas. As atribuições conferidas pela portaria são, em geral, de caráter educativo e preventivo, como as de produção de materiais informativos para combate à desinformação, ou de treinamento midiático para lidar com os novos mecanismos tecnológicos.

Importante mencionar que a atuação administrativa no combate à desinformação certamente se encontra limitada, uma vez que não há ainda lei específica prevendo as hipóteses de atuação dos poderes públicos, tornando-se inviável a aplicação de determinadas sanções ou outros mecanismos regulatórios por parte do poder executivo. Cumpre ainda, por derradeiro, destacar o PL 2630/20, denominado Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, ou, mais frequentemente, como "lei

---

[70] SUPREMO TRIBUNAL FEDERAL. **Ação Direta de Inconstitucionalidade 4.451/DF.** Relator Ministro Alexandre de Moraes. 2018.

[71] MADRUGA, Sidney Pessoa. Propaganda Eleitoral, espécies, propaganda antecipada e propaganda na Internet. In: **Revista Brasileira de Direito Eleitoral RBDE**. ano 5, n. 8, jan./jun. 2013.

[72] Danilo Doneda coloca que, mediante o profiling, "os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma 'metainformação', que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamento e destino de uma pessoa ou grupo." DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

[73] KAISER, Brittany. Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. Harper Collins Brasil. E-book Kindle. 2020.

[74] BRASIL. Tribunal Superior Eleitoral. **Portaria 318 de 30 de Março de 2022.** Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2022/portaria-no-318-de-30-de-marco-de-2022 Acesso em: 6 de Abril de 2022.

das fake news"[75]. Apesar de já contar com quase 2 anos desde o início de sua tramitação, o projeto vem sendo submetido a diversos ajustes por parte do legislador brasileiro, o que é indispensável para a elaboração de um rol de previsões regulamentares que se encontrem constitucionalmente adequadas.

Considerações Finais

Pelo que se demonstrou, sobretudo no tocante ao grau de afetação, é possível conferir que a legislação brasileira, especialmente em relação ao período eleitoral, possui algumas disposições voltadas para o combate às campanhas de desinformação, exigindo que candidatos e partidos cumpram com requisitos que permitam identificar a origem dos fundos e o conteúdo das mensagens publicitárias veiculadas nos ambientes virtuais. Entretanto, como se apurou, a maior parte destas disposições volta-se para a tutela penal, buscando responsabilizar aqueles que dolosamente se utilizam das plataformas digitais para atacar o próprio regime democrático, bem como as instituições, mediante o aniquilamento e a erosão do debate livre e plural, uma vez que este é o objetivo das campanhas de desinformação. A principal consequência é polarização que caracteriza o domínio da politica, mas que se expande de modo acelerado para todas as áreas da vida publica, tornando o consenso uma espécie ficcional em desuso.

Entende-se, em razão disso, que, de qualquer sorte, a coerção penal segue sendo um elemento importante e constitucionalmente adequado, tendo em vista que a Constituição Federal brasileira admite a limitação da liberdade de expressão em casos extremos e específicos, nunca mediante a censura prévia, mas sim em sede de reparação civil ou punição daqueles que cometerem abusos. Para a sanção penal evidentemente se faz necessário a conduta dolosa, intencional, de subversão democrática, se utilizando de mecanismos tecnológicos para campanhas de desinformação.

Exatamente por isso que, apesar de adequada e necessária, a sanção penal prevista em diversas hipóteses pela legislação eleitoral brasileira se apresenta também como insuficiente, uma vez que somente será possível punir quando estiverem presentes todos os elementos necessários para a persecução penal, tema o qual não há espaço para adentrar, mas se faz necessário referir que não se pode buscar proteger a Constituição violando-a, ou seja, mesmo nos casos de violação da legislação eleitoral é necessário que se observe as garantias fundamentais materiais e processuais que envolvem a persecução criminal. Não se pode, sob pena de total contrassenso, adensar no arbítrio para a consolidação da democracia.

Assim, para uma factível mitigação das campanhas de desinformação se faz necessário ir além, buscando mecanismos capazes de compelir a própria arquitetura das redes, a fim de que não sirvam como meios a serem utilizados dessa forma. Outra maneira é apostar em campanhas de educação para a cidadania, notadamente a cidadania digital. Por hora, se faz necessário estabelecer mecanismos regulatórios que componham

[75] BRASIL. Câmara dos Deputados. **Projeto de Lei 2630/20 – Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.** Disponível em: https://www.camara.leg.br/propostas-legislativas/2256735 Acesso em: 6 de Abril de 2022.

um rol capaz de conduzir a atuação das companhias tecnológicas como meios de aprofundamento da democracia e do pluralismo, e não de seu enfraquecimento e derrocada. Obviamente isto importa em mecanismos complexos, envolvendo, v.g., a abertura de uma caixa de pandora que implique na democratização das próprias redes, resultando na transparência de seus processos e decisões, na autenticidade de seus espaços. O ponto de partida já foi encetado, contudo o itinerário se faz na contínua afirmação de um corolário de direitos e de garantias que merecem toda a atenção e zelo, vez que são centrais para o amadurecimento do protagonismo cidadão no contexto brasileiro, trazendo implicações, inclusive, para o âmbito internacional.

Referências

ALEXY, Robert. **Teoria dos Direitos Fundamentais.** 2ª ed. Malheiros. São Paulo. 2014,

BALAGUER CALLEJÓN, Francisco. As Duas Grandes Crises do Constitucionalismo Diante da Globalização no Século XXI. In: **Joaçaba**. v. 19, n. 3, set./dez. 2018.

BALAGUER CALLEJÓN, Francisco. Redes Sociais, Companhias Tecnológicas e Democracia. In: HABERLE, Peter et al. (Orgs). **Direitos Fundamentais, Desenvolvimento e Crise do Constitucionalismo Multinível**. Editora Fundação Fênix. Porto Alegre. 2020.

BRASIL. **Código Eleitoral – Lei 4.737 de 15 de Julho de 1965.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm. Acesso em: 18 set. 2021.

BRASIL. **Lei dos Partidos Políticos – Lei 9.096 de 19 de Setembro de 1995.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9096.htm. Acesso em: 21 set. 2021.

BRASIL. **Lei das Eleições – Lei 9.504 de 30 de Setembro de 1997.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 18 set. 2021.

BRASIL. **Lei 14.192 de 4 de Agosto de 2021.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14192.htm. Acesso em: 20 set. 2021.

BRASIL. Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental 130.** Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605411. Acesso em: 11 ago. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 4.451/DF.** Relator Ministro Alexandre de Moraes. 2018.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 4650/DF**. Relator Ministro Luiz Fux. 2015.

BRASIL. Tribunal Superior Eleitoral. **Recurso Especial Eleitoral 21594/RS.** Relator Ministro Luiz Carlos Madeira. 2004.

BRASIL. Tribunal Superior Eleitoral. **Portaria 318 de 30 de Março de 2022.** Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2022/portaria-no-318-de-30-de-marco-de-2022 Acesso em: 6 de Abril de 2022.

CLÈVE, Clèrmerson Merlin. A Eficácia dos Direitos Fundamentais Sociais. In: **Revista de Direito Constitucional e Internacional.** v. 54. 2006

DEUTSCHLAND. **Lei Fundamental da Alemanha**. Disponível em: https://www.btg-bestellservice.de/pdf/80208000.pdf. Acesso em: 25 ago. 2021.

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

DWORKIN, Ronald. **Levando os Direitos a Sério**. São Paulo. Martins Fontes. 2002.

FELDENS, Luciano. Direitos fundamentais e Direito Penal: garantismo, deveres de proteção, princípio da proporcionalidade, jurisprudência constitucional penal, jurisprudência dos tribunais de direitos humanos. Porto Alegre: Livraria do Advogado, 2008.

FISS, Owen. Free Speech and Social Structure. In: **Iowa Law Review**. n. 71. 1986.

GRIMM, Dieter. **Multiculturalidad y Derechos Fundamentales Trad**: Ignacio Gutiérrez Gutiérrez. Editorial Trotta. Madrid. 2007.

HARTMANN, Ivar; MONTEIRO, Julia. Fake News no contexto de Pandemia e Emergência Social: os Deveres e Responsabilidades das Plataformas de Redes Sociais na Moderação do Conteúdo Online. In: **RDP.** Brasília, v. 17, n. 94, jul./ago. 2020.

HARTMANN, Ivar. A New Framework for Online Content Moderation. In: **Computer Law and Security Review.** n. 36, 2020

HARTMANN, Ivar. Liberdade de Expressão e Capacidade Comunicativa: Um Novo Critério Para Resolver Conflitos entre Direitos Fundamentais Informacionais. In: **Direitos Fundamentais e Justiça. Belo Horizonte**. ano 12, n. 39, jul./dez. 2018.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital.** Rio de Janeiro. Forense. 2020.

KAISER, Brittany. Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. Harper Collins Brasil. E-book Kindle. 2020.

KELLER, Clara Iglesias. Don't Shoot the Message: Regulating Desinformation Beyond Content. In: **Revista de Direito Público**. Brasília, v. 18, n. 99, jul./set. 2021.

MADRUGA, Sidney Pessoa. Propaganda Eleitoral, espécies, propaganda antecipada e propaganda na Internet. In: **Revista Brasileira de Direito Eleitoral RBDE**. ano 5, n. 8, jan./jun. 2013.

MENDES, Gilmar Ferreira. A Doutrina Constitucional e o Controle de Constitucionalidade como Garantia da Cidadania. Declaração de Inconstitucionalidade sem a pronúncia de nulidade no Direito brasileiro. In: **Revista de Direito Administrativo**. Rio de Janeiro, jan./mar. 1994.

PORTUGAL. **Decreto-Lei nº. 319-A/76**. Disponível em: https://dre.pt/home/-/dre/655916/details/maximized. Acesso em: 21 set. 2021.

SARLET, Ingo Wolfgang; HARTMANN, Ivar Alberto Martins. Direitos Fundamentais e Direito Privado: a Proteção da Liberdade de Expressão nas Mídias Sociais. In: **RDU**. Vol. 16. N. 90. Nov-dez 2019. Porto Alegre. 2019.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: BIONI, Bruno et al. **Tratado de Proteção de Dados Pessoais**. Forense. 2021. E-book Kindle.

SARLET, Ingo Wolfgang; SIQUEIRA, Andressa de Bittencourt. Liberdade de Expressão e Seus Limites numa Democracia: O Caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil. In: **Revista de Estudos Institucionais.** v. 6, n. 2, maio/ago. 2020.

O Direito Digital enquanto disciplina jurídica: apontamentos sobre a sua génese no Brasil, o seu conceito e o seu objeto

Duilio Landell de Moura Berni[76]

RESUMO

O presente estudo mostra uma visão histórica da formação do conceito de Direito Digital, passando da Informática Jurídica ao Direito da Informática, com foco mais detido na doutrina jurídica brasileira. O texto é uma adaptação e uma reformulação de parte da tese de doutoramento do autor intitulada "Fundamentos para uma autonomia científica do Direito Digital no ordenamento jurídico brasileiro". Como conclusão, afirma-se que o Direito Digital estuda as relações jurídicas cujo objeto seja o tratamento de dados com a utilização das Tecnologias da Informação e Comunicação (TICs), especialmente com o uso dos meios digitais.

PALAVRAS-CHAVE

Direito Digital, Informática Jurídica, Histórico, Conceito. Objeto.

[76] Doutor em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Advogado e parecerista em Porto Alegre, Brasil. *Curriculum vitae:* http://lattes.cnpq.br/2549693750306775. ORCID: https://orcid.org/0000-0002-7699-7404.

Digital Law as a legal discipline: notes on its geneses in Brazil, its concept and its object

Duilio Landell de Moura Berni

ABSTRACT

This study presents a historical view of the formation of the concept of Digital Law, passing from Legal Informatics to Informatics Law, with a closer focus on Brazilian legal doctrine. The text is an adaptation and a reformulation of part of the author's doctoral thesis entitled Fundamentals for a scientific autonomy of Digital Law in the Brazilian legal system. As a conclusion, Digital Law studies the legal relationships whose object is data processing with the use of Information and Communication Technologies (ICTs), especially with the use of digital media.

KEYWORDS

Digital Law, Legal Informatics, Historic, Concept, Object.

Introdução

O presente texto é uma adaptação e uma reformulação de parte da tese de doutoramento do autor intitulada *Fundamentos para uma autonomia científica do Direito Digital no ordenamento jurídico brasileiro*. Ao longo da pesquisa de doutorado, foi possível verificar que os estudos que buscam descrever e conciliar a relação entre os computadores e o Direito já são realizados há algumas décadas. Tal relação, contudo, permite dois enfoques diversos, mas não excludentes. O primeiro enfoque decorre do contato inicial dos juristas com a informática e, por isso mesmo, foi denominado de Informática Jurídica. Isso ocorreu quando os juristas perceberam que era possível tirar enormes vantagens da utilização dos computadores na sua prática profissional. Pesquisadores, juízes, advogados e membros do Ministério Público logo perceberam que suas atividades poderiam ganhar muito em eficiência e em rapidez, tanto quantitativa, como qualitativamente, com as inúmeras aplicações da informática na vida jurídica.

Em contrapartida, a utilização da informática e dos meios digitais por parcelas cada vez mais significativas das sociedades humanas, por empresas, por corporações e pelos Estados nacionais, vem criando espaço e evidenciando a necessidade do surgimento de um ramo jurídico próprio para pesquisar, compreender, sistematizar e indicar caminhos válidos para a tutela dessas relações, bem como para atender a dificuldades taxonômicas atualmente existentes, que decorrem também da proliferação de normas jurídicas sobre o tema.

Diante da evidência de que o avanço tecnológico é inafastável, as bases teóricas tradicionais necessitam ser revisitadas e novos institutos jurídicos precisam ser aprofundados para que se esteja à altura dessa tarefa que incorpora um novo *modus vivendi*, também chamado de "digitalização da vida", ligado à computação ubíqua. As dificuldades taxonômicas ocorrem, por exemplo, no debate sobre a atribuição (ou não) de uma personalidade jurídica a um computador ou um robô, dotado de um programa de Inteligência Artificial (IA), isto é, enquanto entidade pensante autônoma.

Outrossim, cada vez mais é necessário atentar para a proteção do direito à privacidade no que se refere a dados pessoais e ao seu monitoramento. Esse é, sem dúvida, um dos principais desafios a que são submetidos atualmente os direitos humanos, tanto na sua dimensão internacional como nacional, com o perigo real de uma nova reificação da pessoa humana. É de suma importância, pois, o desenvolvimento de regras e de princípios específicos que conduzam à sua proteção nas mais diversas – e novas – dimensões diante da vulnerabilidade geral dos usuários das Tecnologias da Informação e Comunicação (TICs). O tema guarda ainda íntima relação com as garantias a outros direitos fundamentais, além da proteção dos dados pessoais, como os tradicionais direitos de liberdade e de igualdade.

As TICs, especialmente pela sua arquitetura própria e pelos meios digitais que utilizam, inevitavelmente geram uma nova perspectiva nas relações entre os seres humanos,

nas relações entre os indivíduos e as corporações, nas relações entre as próprias corporações, nas relações entre o Estado e os indivíduos, nas relações entre o Estado e as corporações, e ainda nas relações entre os indivíduos e a tecnologia em si mesma.

Daí a pertinência dos estudos sobre a criação, o conceito e o objeto do Direito Digital. Nesse sentido, na própria gênese do fenômeno aqui descrito, será apresentado também o conceito e uma visão histórica da Informática Jurídica no Brasil, bem como o posterior conceito de Direito Digital.

1. Gênese e Histórico do Direito Digital: da Informática Jurídica ao Direito da Informática

A Informática Jurídica consiste em métodos de utilização prática dos meios informáticos pelos operadores do Direito, sendo esses meios empregados como um instrumento de trabalho no âmbito jurídico. É a informática aplicada ao Direito. Tais métodos de utilização da computação em favor do Direito podem gerar uma infinidade de aplicações, que irão espelhar a criatividade dos próprios operadores jurídicos e dependerão das inovações tecnológicas disponíveis.

A criação do termo "informática" remonta à metade do século XX. Nas décadas entre 1970-1990, o termo ganhou popularidade no mundo ocidental, inclusive como sinônimo de Ciência da Computação. Hoje em dia, o termo rivaliza em uso com a sigla TI (Tecnologias da Informação).[77] A trajetória da informática no ambiente jurídico e acadêmico brasileiro tem como um dos seus pontos iniciais um curso de Informática Jurídica que foi ministrado pelo brasilianista e professor italiano Mario Giuseppe Losano, evento que ocorreu na Faculdade de Direito de São Paulo, no Largo de São Francisco, em 1973, a convite do Professor Miguel Reale.[78]

Esse professor italiano realizou, no final do século XX, um intercâmbio consolidado com o Brasil, com passagens frequentes pelo país sul-americano, publicando uma série de artigos científicos, concedendo entrevistas e ministrando palestras. Em sua passagem por Porto Alegre, publicou artigos na Revista da Procuradoria-Geral do Estado do Rio

[77] Um breve histórico dessa transformação é apresentado por Denis Alcides Rezende, nos seguintes termos: "Na década de 1960, o tema tecnológico que rondava as organizações era o 'processamento de dados'. Nessa época, a maioria das empresas direcionava os recursos para o processamento centralizado de dados em mainframes (grandes computadores) e para os sistemas de controles operacionais, tais como faturamento, estoque, folha de pagamento, finanças e contabilidade. [...] Aos poucos, porém, as empresas foram se sensibilizando para a importância da informação na gestão de negócios. Contagiadas pela 'informática', que passa a substituir o tradicional 'processamento de dados', as empresas superaram resistências e incorporaram essa nova ferramenta empresarial. Com a 'informática', as empresas integraram os seus sistemas, mesmo com algumas redundâncias. Na atualidade, a 'informática' se transforma em 'tecnologia da informação' (TI), integrando os seus emergentes e modernos recursos. A TI pode ser conceituada como o conjunto dos recursos tecnológicos e computacionais para guarda de dados, geração e uso da informação e de conhecimentos". *Vide* REZENDE, Denis Alcides. A evolução da tecnologia da informação nos últimos 45 anos. **Revista FAE BUSINESS**, Curitiba, n. 4. dez. 2002. Disponível em: <https://img.fae.edu/galeria/getImage/1/16578659447373246.pdf>. Acesso em: 28 abr. 2021.

[78] LOSANO. Mario G. A informática jurídica vinte anos depois. Revista dos Tribunais, São Paulo, v. 715, p. 350-367, maio 1995. p. 350.

Grande do Sul, com temas inovadores como "Lexicografia computacional e informática jurídica"[79] e "A lei alemã de proteção de dados".[80]

Como o resultado da compilação dessas aulas e seminários ministrados na Universidade de São Paulo, foi editado um livro de Mario Giuseppe Losano, obra de referência que de certa forma inaugurou o tema nas letras jurídicas brasileiras, conforme o seu "Lições de Informática Jurídica", de 1974.[81] A referida obra contém, dentre outros temas, noções de informática e de cibernética, bem como noções básicas de programação e processamento de dados para juristas.

Também Miguel Reale, em sua clássica obra *Lições preliminares de direito*,[82] já dedicava, no final do século XX, um tópico para a Juscibernética, considereda por ele como gênero do qual a Informática Jurídica seria subespécie, nos seguintes termos:

> […] no quadro da renovação dos conhecimentos jurídicos, está se constituindo a Cibernética Jurídica ou Juscibernética, que se propõe a compreender a conduta jurídica segundo modelos cibernéticos (o comportamento humano em termos de "comportamento" das máquinas) e a colocar à disposição imediata dos juristas os recursos dos computadores eletrônicos, por exemplo, na tarefa legislativa, na ordenação polivalente dos dados jurídicos e a realização rigorosa de cálculos resultantes da aplicação das regras jurídicas onde seja possível a quantificação.
> Parte relevante da Juscibernética é a Informática Jurídica, que delineia novas e fecundas perspectivas no sentido de fornecer ao jurista um "banco dados". É preciso, porém, evitar deformações incabíveis quanto à redução final do "qualitativo" ao "quantitativo", ou à substituição da apreciação do juiz pela memória decisória dos autômatos… [83]

Essa visão utilitarista da informática em favor do Direito manteve-se ao longo dos anos, e novas ferramentas foram concebidas para ajudar os juristas, sobretudo com o advento das TICs.[84] Tal qual o conceito de Informática Jurídica anteriormente apresentado, também emprega-se hoje a expressão Legal Technology, ou Legal Tech para descrever o mesmo fenômeno. Para Wolfganf Hoffmann-Riem, Legal Technology "refere-se ao uso da tecnologia da informação nos campos jurídicos de atividades como assessoria

---

[79] LOSANO. Mario G. *Lexicografia computacional e informática jurídica*. **Revista da Procuradoria-Geral do Estado,** Porto Aelgre, v. 10, n. 26, p. 67-71, 1980.

[80] LOSANO. Mario G. *A lei alemã de proteção de dados*. **Revista da Procuradoria-Geral do Estado**, Porto Alegre, v. 11, n. 19, p. 11-22, 1981.

[81] LOSANO, Mario G. **Lições de informática jurídica**. São Paulo: Resenha Tributária, 1974.

[82] REALE, Miguel. **Lições preliminares de direto**. 21. ed. rev. atual. ampl. São Paulo: Saraiva, 1994.

[83] REALE, Miguel. **Lições preliminares de direto**. 21. ed. rev. atual. ampl. São Paulo: Saraiva, 1994. p. 331-332.

[84] Nesse sentido, Giovanni Ziccardi, que leciona, em livre tradução: "O coração da informática jurídica sempre foi essencialmente prático e a informática jurídica é entendida, na era moderna, pela maior parte dos estudiosos, como um meio para ilustrar as teorias da informação e da comunicação, com o fim de constituírem um instrumento de trabalho simples e imediato para os juristas.". Cf. ZICCARDI, Giovanni. Informatica giuridica. *In:* ZICCARDI, Giovanni; PERRI, Pierluigi (org.). **Dizionario legal tech**. Milano: Giuffrè Francis Lefebvure, 2020. p. 520.

jurídica, jurisprudência, na aplicação do Direito, mas também no processo legislativo.".[85] De maneira similar, Giulio Messori assim define Legal Tech: "termo usado para identificar aplicações e soluções tecnológicas, especialmente sob

a forma de software, dedicados a digitalizar, automatizar, racionalizar ou simplificar atividades e processos de trabalho no âmbito das profissões legais".[86]

Ainda ao lado da Informática Jurídica, desponta também uma disciplina que vem sendo chamada de Jurimetria, que é estatística aplicada ao Direito, ou, noutras palavras, a análise quantitativa de dados resultantes da atividade jurídica, como a produção legislativa e a jurisprudência. Newton de Lucca leciona que o termo Jurimetria foi cunhado por Lee Loevinger, na década de 1960, quando ele estava estudando o comportamento de legisladores e de juízes na busca de soluções para problemas jurídicos.[87] Marcelo Guedes Nunes aponta que a Jurimetria é fundada em três pilares básicos: 1) o jurídico; 2) o estatístico e 3) o computacional.[88]

Nesta relação entre as tecnologias e o Direito, Giovanni Ziccardi apresenta duas divisões bem marcadas dentro da Informática Jurídica. A primeira decorre da própria evolução tecnológica, com o advento da internet, na qual se passa de uma "Informática Jurídica Tradicional", essencialmente estática e documental, para uma "Nova Informática Jurídica", aberta, dinâmica e com amplo acesso on-line aos bancos de dados.[89] A segunda divisão decorre de um desdobramento entre a Informática Jurídica e o Direito da Informática, nos seguintes termos:

> Uma segunda bipartição tradicional, na relação entre a informática e o direito, é aquela entre informática jurídica em sentido estrito e os direitos (ou direito) da informática.
>
> A disciplina que diz respeito aos direitos da informática se caracteriza por não ser uma disciplina única e homogênea, mas sim por reunir, sob uma única denominação um feixe de subdisciplinas que se podem reconectar a uma ou mais disciplinas relevantes (pode-se pensar, por exemplo, no direito penal da informática, no direito tributário da informática, no direito público da informática).
>
> Normalmente, a atividade de ensino e investigação na área dos direitos

---

[85] Cf. HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022. p. 183. Para uma perspectiva de aplicação da IA à jurisdição brasileira, veja-se: MACHADO, Fernanda de Vargas; COLOMBO, Cristiano. Inteligência artificial aplicada à atividade jurisdicional: desafios e perspectivas para sua implementação no Judiciário. **Revista da Escola Judicial do TRT 4**. Porto Alegre, v. 3. n. 5. p. 117-141, jan./jun. 2021.

[86] Cf., em livre tradução, MESSORI, Giulio. Legal tech. In: ZICCARDI, Giovanni; PERRI, Pierluigi (org.). Dizionario legal tech. Milano: Giuffrè Francis Lefebvure, 2020. p. 584-585.

[87] Cf. DE LUCCA, Newton. Títulos e contratos eletrônicos: o advento da informática e suas consequências para a pesquisa jurídica. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coord.). **Direito & internet**: aspectos jurídicos relevantes. 2 ed. São Paulo: Quartier Latin, 2005. p. 50-51.

[88] NUNES, Marcelo Guedes. O que é jurimetria? **Revista de Direito Bancário e do Mercado de Capitais**. v. 62. p.253-260. Out. - Dez. 2013. p. 4. Para aprofundamento do tema, veja-se ainda do mesmo autor o livro "Jurimetria: como a estatística pode reinventar o Direito". Cf. NUNES, Marcelo Guedes. **Jurimetria**: como a estatística pode reinventar o direito. 2 ed. São Paulo: RT, 2019. Um estudo de caso baseado na Jurimetria, com metodologia de pesquisa bem definida, é realizado por Dierle Nunes e Fernanda Amaral Duarte, buscando entender as condenações por danos morais em decorrência do cadastro indevido nos órgãos de proteção ao crédito, em decisões proferidas pelo Tribunal de Justiça de Minas Gerais no ano 2018. Cf. NUNES, Dierle; DUARTE, Fernanda Amaral. Jurimetria e tecnologia: diálogos essenciais com o direito processual. **Revista de Processo**. v. 299. São Paulo: RT Jan. 2020. p. 405-448.

[89] ZICCARDI, Giovanni. **Manuale breve:** informatica giuridica. Milano: Giuffrè, 2006. p. 72-73.

> da informática é conduzida por especialistas da disciplina que prevalece, até porque, em alguns casos, os ramos do direito estão muito distantes uns dos outros.
>
> Uma outra distinção poderia ser aquela entre "direitos da informática" e "direitos com informática", significando o primeiro como regulamentação legal para atividades de informática e o último como atividades regulamentadas pelo Direito com um forte componente de informática. Pense, por exemplo, na pirataria de computador como pertencente à primeira categoria e, na segunda, um crime cometido por meio do correio eletrônico.[90]

Daí a visão do fenômeno como as duas faces de uma mesma moeda, sendo a Informática Jurídica como a aplicação das TICs ao Direito e o Direito da Informática como a aplicação do Direito às TICs. Esse entedimento revela a noção inicial do fênomeno "Direito da Informática", com destaque para a sua característica de disciplina heterogênea, que não seria mais do que uma disciplina conduzida por especialistas noutros ramos do Direito quando houvesse algum aspecto da informática envolvido.

Nas letras jurídicas brasileiras, o Direito da Informática foi criando espaço e se consolidando a partir do final do século XX. Uma das primeiras obras sobre o tema é o livro *Direito de Informática*, de Liliana Minardi Paesani, com a sua primeira edição lançada em 1998. De maneira similar a Giovanni Ziccardi, ela refere que a "Informática do Direito" concebe o Direito como objeto da informática, ao passo que, no "Direito de Informática", é a informática que é tratada como objeto do Direito.[91] Na décima edição da obra, do ano de 2015, Liliana Minardi Paesani propõe uma "nova reflexão", para que seja repensando o conceito de direito digital, assumindo tacitamente uma identidade entre as expressões "Direito da Informática" e "Direito Digital".[92]

Ricardo Lorenzetti, no primeiro capítulo de sua obra *Comércio eletrônico*, capítulo dedicado à formulação de uma "teoria geral", busca diferenciar as expressões "Direito informático", "Direito do espaço virtual" e "Direito virtual".[93] Ocorre que as descrições des-

---

[90] Texto em livre tradução do seguinte original: "Una seconda bipartizione tradizionale, nel rapporto tra l'informatica e il diritto, è quella tra informatica giuridica in senso stretto e diritti (o diritto) dell'informatica. La disciplina che riguarda i diritti dell'informatica si caratterizza per non essere una disciplina unica e omogenea, ma per riunire, sotto un'unica denominazione, un fascio di sotto-discipline che si possono ricollegare a una o più discipline rilevanti (si può pensare, ad esempio, al diritto penale dell'informatica, al diritto tributario dell'informatica, al diritto pubblico dell'informatica). Solitamente, l'attività didattica e di ricerca in tema di diritti dell'informatica è condotta da specialisti della disciplina «prevalente», anche perchè, in alcuni casi, i rami del diritto sono molto lontani tra loro. Una distinzione ulteriore potrebbe essere quella tra «diritti dell'informatica» e «diritto con l'informatica», intendendo i primi come regolamentazioni giuridiche di attività informatiche, e i secondi come attività regolate dal diritto con una forte componente informatica. Si pensi, ad esempio, come appartenente alla prima categoria la pirateria informatica, e alla seconda un reato commesso usando la posta elettronica.". (ZICCARDI, Giovanni. Manuale breve: informatica giuridica. Milano: Giuffrè, 2006. p. 73-74.).

[91] PAESANI, Liliana Minardi. **Direito de informática**: comercialização e desenvolvimento internacional do software. 6. ed. atual. São Paulo: Atlas, 2009. p. 7.

[92] PAESANI, Liliana Minardi. **Direito de informática**: comercialização e desenvolvimento internacional do software. 10. ed. São Paulo: Atlas, 2015. p. XI e p. 89.

[93] Cf. "Direito informático. Acentua os computadores e o processamento da informação, e, sobretudo, a possibilidade de aplicar a lógica formal, a análise quantitativa e todo corpo cognoscitivo desenvolvido pela informática no campo jurídico. [...] Direito do espaço virtual. Aqui, o propósito fundamental não é aplicar a computação ao Direito, mas sim o Direito à computação. O mundo virtual cresceu tanto que alcançou o status de objeto regulatório; em vista disso, surgem problemas de toda índole na área virtual. Direito virtual.

ses fenômenos pelo referido autor carecem de precisão e pecam por não conseguir circunscrever seus objetos. O que ele denomina como "Direito informático", por exemplo, é o que vem sendo denominado pela maior parte da doutrina já referenciada no presente texto como Informática Jurídica.

Por outro lado, as fronteiras entre as definições apresentadas de "Direito do espaço virtual" e de "Direito virtual" não são suficientemente demarcadas por Ricardo Lorenzetti, revelando uma identidade de conteúdos entre o "espaço virtual" e o "virtual" – no modo por ele definidos. Concorda-se com esse autor, contudo, quando ele afirma que hoje utilizam-se "muitas denominações distintas" para referir um único fenômeno, isto é, o do Direito frente ao novo paradigma digital.[94]

Danielle Mendes Thame Denny apresenta a seguinte conceituação para o Direito da Informática, em seu compêndio *Internet Legal:*

> Direito da Informática, também chamado Direito Digital ou Cyber Direito, tem como objeto fatos jurídicos que ocorrem em meio eletrônico, ou seja que contenham, no suporte fático, um componente da informática (equipamento eletrônico, máquina computacional, Internet, Intranet, programa, algorítimo, rede social etc).[95]

Vê-se que a autora usa indistintamente as expressões "Direito da Informática" e "Direito Digital" para designar um mesmo fenômeno, o que indica mais um caso de indecisão por parte da doutrina jurídica brasileira na abordagem do tema ora em exame. Quanto ao objeto de estudo do Direito da Informática, conforme descrito por ela, a crítica que se faz é no sentido de ser um objeto por demais amplo. Esse objeto – segundo o entendimento manifesto no presente estudo – escapa ao foco da disciplina do Direito Digital, pois, nas palavras de Danielle Mendes Thame Denny, bastaria a existência de um computador ou de um *software* no suporte fático de um fato jurídico para que a matéria se tornasse de seu interesse. Ocorre que inúmeras situações irão fugir a essa descrição muito abrangente. Pense-se, por exemplo, na compra de um *software* pela Administração Pública. Embora haja no suporte fático dessa contratação um elemento de TI, a disciplina de tutela dessa relação jurídica é o Direito Administrativo e a sua regulamentação se dá nos termos da Lei de Licitações e Contratos Administrativos.[96]

Com o emprego deste termo, faz-se referência ao fato de que o Direito deve adotar o paradigma digital. Utilizam-se muitas denominações distintas para referir este fenômeno, mas basicamente consiste na idéia de que a teoria dos sistemas, a lógica formal, a teoria do caos, a tecnologia digital, constituem um corpo cognoscitivo autônomo que demanda a criação de uma nova ordem jurídica.". (LORENZETTI, Ricardo L. Comércio eletrônico. Trad. Fabiano Menke, notas Cláudia Lima Marques. São Paulo: RT, 2004. p. 72-73)

94 LORENZETTI, Ricardo L. **Comércio eletrônico**. Trad. Fabiano Menke, notas Cláudia Lima Marques. São Paulo: RT, 2004. p. 73.

95 DENNY, Danielle M. T. Internet legal. Piracicaba: Imagens DD, 2016. Disponível em: <https://docero.com.br/doc/xve8c1s>. Acesso em 03 dez. 2021. p. 7.

96 Veja-se o seguinte dispositivo da referida legislação: Lei nº 14.133/2021. Das Compras. Artigo 43. O processo de padronização deverá conter: I – parecer técnico sobre o produto, considerados especificações técnicas e estéticas, desempenho, análise de contratações anteriores, custo e condições de manutenção e garantia; II – despacho motivado da autoridade superior, com a adoção do padrão; III – síntese da justificativa e descrição sucinta do padrão definido, divulgadas em sítio eletrônico oficial. [...] § 2º As contratações de soluções baseadas em software de uso disseminado serão disciplinadas em regulamento que defina processo de gestão estratégica das contratações desse tipo de solução.

Outra denominação empregada inicialmente para descrever o fenômeno ora em estudo é "Direito Eletrônico". Em 2012, de maneira pioneira, Tarcisio Teixeira lança a primeira edição do seu "Curso de Direito e Processo Eletrônico",[97] obra que foi revista e ampliada, conforme o surgimento de novas legislações sobre o tema e, a partir da quinta edição, por sugestão da editora, passou a ser denominada como *Direito Digital e Processo Eletrônico*.[98] Nela são abordados diversos temas, em profundidade, como: a internet e seus aspectos operacionais, o Marco Civil da Internet a LGPD, o teletrabalho, a Internet das Coisas, os crimes de informática, a tributação na internet, a informatização do processo judicial, dentre tantos outros.

Quanto ao objeto do presente estudo, vejam-se alguns exemplos de outras terminologias utilizadas que gravitam em seu entorno: Direito da Informação ou Direito Informacional;[99]Direito Cibernético ou Direito do Ciberespaço[100] e Direito Virtual.[101] Em língua inglesa, também para descrever o mesmo fenômeno, utilizam-se as expressões *Cyber Law,*[102] *Cyberspace Law,*[103] *Internet Law*[104] e *Information Technology (IT) Law*.[105] Em língua

---

[97] Cf. "[...] preferimos usar 'direito eletrônico', tendo em vista o emprego recorrente do vocábulo 'eletrônico' em expressões como 'comércio eletrônico' e 'correio eletrônico'. Além do mais, a palavra 'eletrônico' está relacionada à eletrônica, que é aquela parte da física que trata de circuitos elétricos; sendo que a comunicação de dados via computador se faz por meio de impulsos elétricos, o que a caracteriza como comunicação eletrônica. Por essa razão, justifica-se o adjetivo eletrônico para a comunicação gerada por impulsos elétricos, seja um contrato ou não. (TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 3. ed. atual. ampl. São Paulo: Saraiva, 2015. p. 22).

[98] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020. p. 30. Nesse ponto, mais uma vez, manifesta-se a indecisão inicial por parte da doutrina quanto à adoção de uma determinada terminologia para identificar o fenômeno objeto desta tese, com a posterior convergência para uma denominação que vem sendo considerada como mais usual, isto é, a expressão Direito Digital.

[99] Denominação usada por SIQUEIRA JÚNIOR, Paulo Hamilton. Direitos humanos e cidadania digital. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015. p. 171-185. v. 1: Marco Civil da Internet (Lei n. 12.965/2014). p. 179. Ele ainda destaca o surgimento da cidadania no ambiente informacional (a "cidadania digital") e o seu papel fundamental para a construção da própria democracia. p. 180-181.

[100] Cf. "O direito do ciberespaço, por seu turno, é o conjunto de leis, regulamentações em geral e práticas contratuais de todos os tipos e níveis, que envolvam a utilização e funcionamento de redes de software e computadores. É também chamado 'direito online', debatido nos Estados Unidos desde 1985, como o objetivo de se estabelecerem regras para a comunicação, os negócios e o uso em geral das redes de computadores.". (CERQUEIRA, Tarcisio Queiroz. **Software**: lei, comércio, contratos e serviços de informática: manual de utilização para empresários de software e serviços, profissionais de informática e advogados. Rio de Janeiro: Esplanada, 2000. p. 235).

[101] Cf. "O Direito virtual é o direito que nasce das práticas virtuais, mas também é o direito positivo que possa ser aplicado ao virtual. Ainda compreende o direito ao ciberespaço, pois que também recobre o direito à informação. Essa nova ramificação jurídica corresponde ao conjunto de normas que visam tutelar as relações humanas e as violações comportamentais em ambientes digitais. Isto é, se com o uso da tecnologia, as pessoas enviam e recebem informações, realizam negócios, emitem opiniões etc., devem existir regras e princípios que orientem a conduta nesse meio.". (NOVO, Benigno Núñez. Direito virtual. **Boletim Jurídico**, v. 19, n. 1028, ago. 2019. Disponível em: <https://www.boletimjuridico.com.br/artigos/direito-e-internet/4484/direito-virtual>. Acesso em: 28 abr. 2021).

[102] Cf. GRABOWSKI, Mark; ROBINSON, Eric P. **Cyber law and ethics**: regulation of the connected world. New York: Routledge, 2021.

[103] Cf. KU, Raymond S. R. **Cyberspace law**: cases and materials. New York: Wolters Kluwer, 2016.

[104] Cf. REED, Chris. Internet law: text and materials. 2. ed. Cambridge: Cambridge University Press, 2004.

[105] Cf. LLOYD, Ian J. **Information technology law**. 6 ed. Oxford: Oxford University, 2011.

francesa, utiliza-se a expressão *Droit du Numérique*.[106] Em língua italiana, com foco ainda mais fechado e mais específico, Ugo Ruffolo apresenta obra direcionada aos estudos do chamado *Diritto dell'Intelligenza Artificiale*.[107]

Uma outra denominação utilizada, que se considera muito pertinente para caracterizar esse encontro do Direito com as TICs, é Direito das Tecnologias da Informação e Comunicação (DTIC), já que se revela como uma denominação ampla, abarcando tecnologias atuais e futuras. A denominação DTIC, desse modo, não representa um único formato tecnológico, mas engloba todos os formatos possíveis das TICs.[108] Ocorre que essa é uma denominação pouco usual, revelando baixa adesão pela doutrina jurídica brasileira.[109]

Computação, informática, TI e TICs são termos cuja origem remontam a épocas diversas, mas que, muitas vezes, têm sido usados como sinônimos diante de suas relações de pertinência e marcadas intersecções. E, como o próprio nome já anuncia, a chamada Revolução Digital consagrou a excelência do formato digital para a realização da comunicação de informações.[110]

A crítica que se faz é que o próprio termo "digital" está vinculado à tecnologia atualmente preponderante.[111] Estudos importantes já começam a ser conduzidos no sentido de se repensar o próprio dígito binário, o que se daria numa reinvenção com elementos matemáticos provenientes da física quântica.[112] Um dígito, na teorização da computação quântica, poderia assumir o valor de "zero", de "um" e de "zero e um" ao mesmo tempo, numa superposição desses dois valores, no que se convencionou chamar de "*qubit*", isto é, "*bit* quântico".

Portanto, na escolha da denominação da disciplina, seria mais adequado não se ficar atrelado a qualquer tipo específico de tecnologia, já que as inovações tecnológi-

---

[106] Cf. PELLEGRINI, François; CANEVET, Sébastien. Le droit du numérique: une histoire à préserver. Vers un Musée de l'Informatique et de la Société Numérique en France. **Conservatoire National des Arts et Métiers**, Nov. 2012, Paris, France. pp.61-76. Disponível em <hal.inria.fr/hal.-00768912>. Acesso em 04 dez. 2021.

[107] RUFFOLO, Ugo (Org). XXVI Lezioni di Diritto dell'Intelligenza Artificiale. Turim: Giappichelli, 2021.

[108] Em língua portuguesa, por exemplo, a expressão DTIC é utilizada no seguinte estudo: MARTINS, A. G.; MARQUES, J. A. Garcia; DIAS, Pedro Simões. Cyberlaw em Portugal: o direito das tecnologias da informação e comunicação. Lisboa: Centro Atlântico, 2004.

[109] Não fosse essa baixa adesão por parte da doutrina jurídica brasileira, nos termos anteriormente apresentados, a denominação DTIC seria a tecnicamente mais adequada.

[110] Sobre esta revolução impulsionada pelos avanços tecnológicos, veja-se o debate entre os seguintes autores: LEMOS, Ronaldo; DI FELICE, Massimo. **A vida em rede**. Campinas: Papirus 7 Mares, 2014.

[111] Nas palavras de Wolfgang Hoffmann-Riem, "O termo 'digitalização' refere-se inicialmente apenas às tecnologias da informação específicas que processam dados digitais e às infraestruturas (*software e hardware*) criadas para as tecnologias digitais. No entanto, o termo também representa a mudança fundamental nas condições de vida desencadeada pela sua utilização em todo o mundo.". (HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022. p. 01).

[112] Cf. McMAHON, David. **Quantum computing explained**. New Jersey: John Wiley, 2008. p. 11-12. Ainda sobre os possíveis benefícios do processamento de dados via computadores quânticos veja-se, por exemplo, HENDERSON, M.; GALLINA, J.; BRETT, M. Methods for accelerating geospatial data processing using quantum computers. **Quantum Machine Intelligence,** v. 3, n. 4, 2021.

cas, conforme exposto anteriormente, não pedem licença para se consolidar, subjugando, e, muitas vezes, encaminhando para museus as tecnologias que outrora foram consideradas soberanas e que rapidamente se tornaram obsoletas.[113]

Em síntese do que foi apresentado, o que se observa é que há uma variedade muito grande de nomenclaturas, com focos muito próximos e roupagens similares de um mesmo fenômeno. No Brasil, a recente inserção acadêmica do Direito da Informática, com não mais de algumas décadas de existência, já vem operando uma transmutação para a denominação "Direito Digital", que tem se manifestado, atualmente, como a mais usual para designar o estudo das relações jurídicas cujo objeto seja o tratamento de dados com a utilização das TICs.

A consagração do uso de uma determinada terminologia esconde mistérios que esta pesquisa não se propõe a investigar. Todavia, veja-se que, no Brasil, a expressão "Direito Digital" já foi até mesmo adotada pelo Ministério da Educação (MEC), pela sua Câmara de Educação Superior do Conselho Nacional de Educação, conforme a sua inclusão dentre as disciplinas de formação técnico-jurídica do Projeto Pedagógico do Curso de Graduação em Direito, nos termos da Resolução nº 2, de 19 de abril de 2021, do referido ministério.[114] Direito Digital, portanto, é a nomenclatura que o presente estudo acadêmico rende adesão, com a ressalva de entender que seria mais adequada a expressão Direito das Tecnologias da Informação e Comunicação (DTIC) para denominar o fenômeno ora em exame, expressão essa que não será adotada apenas por não ser de uso corrente na literatura jurídica brasileira atualmente.

Assim, conforme será apresentado no seguinte tópico, o entendimento defendido no presente estudo científico é no sentido de que a bipartição entre a Informática Jurídica e o Direito da Informática já revela, no ordenamento jurídico brasileiro, um conjunto sistematizado de normas que dá identidade a uma disciplina jurídica autônoma, disciplina essa que se denomina como Direito Digital.

---

[113] Nesse sentido, Sidney Bittencourt, que afirma: "Com o passar dos anos, as mudanças propiciadas pela evolução tecnológica são cada vez maiores, mais rápidas e mais surpreendentes. As transformações no campo da chamada Tecnologia da Informação - TI ocorrem de tal forma que se pode afirmar ser praticamente impossível o acompanhamento *pari passu* de todo o processo evolutivo. Vivemos em plena Era da Informação, que teve início na década de 1990.". In: BITTENCOURT, Sidney. **Licitação de tecnologia da informação**: contratações de bens e serviços de informática e automação. Leme: J. H. Mizuno, 2015. p. 29-30. Também de maneira similar, afirmando que a boa técnica legislativa recomenda que as normas jurídicas não deveriam deter-se em uma tecnologia específica: LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Thomson Reuters, 2019. p. 63.

[114] Cf. BRASIL. Ministério da Educação. Conselho Nacional de Educação. Câmara de Educação Superior. **Resolução nº 2**, de 19 de abril de 2021.Republicada no Diário Oficial da União de 20 abr. 2021. Artigo 5º O curso de graduação em Direito, priorizando a interdisciplinaridade e a articulação de saberes, deverá incluir no PPC [Projeto Pedagógico do Curso], conteúdos e atividades que atendam às seguintes perspectivas formativas: [...] II - Formação técnico-jurídica, que abrange, além do enfoque dogmático, o conhecimento e a aplicação, observadas as peculiaridades dos diversos ramos do Direito, de qualquer natureza, estudados sistematicamente e contextualizados segundo a sua evolução e aplicação às mudanças sociais, econômicas, políticas e culturais do Brasil e suas relações internacionais, incluindo-se, necessariamente, dentre outros condizentes com o PPC, conteúdos essenciais referentes às áreas de Teoria do Direito, Direito Constitucional, Direito Administrativo, Direito Tributário, Direito Penal, Direito Civil, Direito Empresarial, Direito do Trabalho, Direito Internacional, Direito Processual; Direito Previdenciário, Direito Financeiro, Direito Digital e Formas Consensuais de Solução de Conflitos. [Grifou-se].

2. Conceito de Direito Digital e o seu objeto

Conforme os termos do tópico anterior, entende-se o Direito Digital como aquela disciplina originada nos estudos de Direito da Informática, decorrendo o Direito Digital da própria evolução tecnológica. O ponto de virada dessa evolução foi o advento da internet, por meio do qual se consagrou a utilização das TICs e o seu formato digital.

Uma obra pioneira e paradigmática no Brasil é o livro de Patricia Peck Pinheiro, "Direito Digital", lançado em 2002[115] e que, ao longo de sete edições, revisadas e atualizadas, mais que dobrou de tamanho em 20 anos, incorporando e apresentando inovações tecnológicas, bem como a nova legislação sobre a matéria. Assim ela define o Direito Digital:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.).[116]

Alan Moreira Lopes, em obra conjunta com Keila dos Santos e Tarcisio Teixeira, assim define o Direito Digital:

> Especialidade da ciência jurídica que regula quaisquer interações sociais organizadas ou realizadas em meio eletrônico, mediante normas que consideram o desenvolvimento tecnológico e cujas sanções restabelecem a paz social no âmbito virtual ou real.[117]

Já o notável trabalho de Wolfgang Hoffmann-Riem, trazido à língua portuguesa por Italo Fuhrmann, em 2021, intitulado *Teoria Geral do Direito Digital*,[118] apresenta uma visão transversal do fenômeno e noções básicas de alguns conceitos tecnológicos como algoritmos, Inteligência Artificial (IA) e *Big Data*. Apesar do título da obra, entende-se que ela não pode ser considerada como uma verdadeira "teoria geral", já que, inclusive como o próprio autor reconhece, tem caráter exemplificativo, e não estrutural, diante da amplitude da área temática, demonstrando "o quão diversos são os desafios para o Direito que decorrem da digitalização".[119]

Portanto, pelo caráter exemplificativo desse livro, que apresenta noções básicas das tecnologias digitais, identificando tipos e desafios específicos, sem, contudo, adentrar em estruturas principiológicas e tampouco em conceitos jurídicos estruturantes, entende-

---

[115] PECK, Patricia. **Direito digital**. São Paulo: Saraiva, 2002.

[116] PINHEIRO, Patrícia. Peck. **Direito Digital**. 7 ed. rev. ampl. atual. São Paulo: Saraiva, 2021. p. 26. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 06 nov. 2021.

[117] LOPES, Alan Moreira; SANTOS, Keila; TEIXEIRA, Tarcisio. **Direito digital**: teoria e prática. São Paulo: Tirant lo Blanch, 2021. p. 72.

[118] A primeira edição da obra é do ano de 2021. Cf. HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. Rio de Janeiro: Forense, 2021.

[119] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022. p. 8-9.

se que ele apresenta alguns elementos, fundamentais, diga-se de passagem, para a construção de uma "teoria geral do Direito Digital", não se configurando a obra, com a devida vênia, numa teorização completa do fenômeno, a par do título que foi elegido.

Inegável é, contudo, a enorme contribuição que a referida obra dá à Ciência Jurídica. Wolfgang Hoffmann-Riem expõe de maneira aguda alguns dos desafios a que estão submetidos todos os sistemas jurídicos atuais, em escala global, diante da própria ubiquidade das tecnologias. Além disso, esses desafios, os riscos e as dificuldades pelas quais passam atualmente os sistemas jurídicos são comparáveis e confrontáveis. O autor afirma, contudo, que, a despeito dessa característica global, as respostas a tais inquietudes – ao menos num primeiro momento – devem ser buscadas nos próprios ordenamentos jurídicos nacionais, a não ser que as soluções sejam fornecidas em tratados internacionais ou mesmo em tratados globais.[120]

Assim, para consolidar o objeto de pesquisa do presente estudo, entende-se o Direito Digital como aquele ramo do Direito que estuda as relações jurídicas cujo objeto seja o tratamento de dados com a utilização das TICs, especialmente com o uso dos meios digitais.[121]

Quanto ao primeiro elemento definidor do Direito Digital, a relação jurídica, entende-se que os seus marcos teóricos são, ainda, aqueles gestados desde a Escola Alemã da Pandectística, no século XIX,[122] nos quais há a presença de dois sujeitos, de um suporte fático e de um vínculo de atributividade que une esses sujeitos.[123]

---

[120] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022. p. 08.

[121] É dito "especialmente com o uso dos meios digitais", já que o formato atualmente dominante e preponderante pelo qual as TICs se manifestam é o formato digital. Conforme já fora apontado, o próprio digito binário já está sendo repensado em estudos de fôlego que envolvem a computação quântica.

[122] A Escola Pandectística, sob as premissas já definidas pela Escola Histórica do Direito, busca construir uma teoria sistemática do Direito Privado, fundada em fontes do Direito Romano (o Corpus Iuris Civilis em particular) e nos dogmas da sacralidade da propriedade privada e da autonomia da vontade individual. Seus principais expoentes foram Friedrich Puchta e Bernhard Windscheid. Cf. PANDETTISTICA. In: ENCICLOPEDIA del diritto. Milano: Garzanti. 2001. Ainda sobre a Pandectística, ensina Willis Santiago Guerra Filho: "1.4. Franz Wieacker, abordando em sua monumental História do direito privado o tema "pandectística e positivismo científico" (§ 28), coloca que, apesar da aparência do programa daquela manifestação tardia da Escola Histórica, ela terminou por contribuir menos para o estudo histórico do Direito do que para a construção de uma sistematização conceitual, iniciada já pelo jusracionalismo, tendo como base a civilística do direito comum europeu. Essa sistemática, posteriormente, é transposta para o direito público por juristas como Jhering, Gerber, Laband e, especificamente, para o direito processual por Bülow, Wach, Goldschmidt etc. No plano epistemológico, seguindo a orientação do programa de Savigny, Puchta propõe a chamada "jurisprudência (= ciência jurídica) dos conceitos", legitimando a dedução de normas e a construção do Direito, desenvolvendo conceitos por uma lógica imanente ao sistema jurídico. Windscheid, o expoente máximo da pandectística, por seu turno, defendia a aplicação do Direito utilizando elementos exclusivamente jurídicos, com a separação de outros quaisquer, de ordem política, econômica, ética etc. Eis aí a idéia central do positivismo científico, a qual remonta à rigorosa diferenciação operada por Kant entre as ordens moral e jurídica, donde resulta o formalismo como princípio retor da prática científica.". (GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini (Colab.). Teoria da ciência jurídica. 2 ed. São Paulo: Saraiva, 2009. p. 40).

[123] Essa noção de relação jurídica é apresentada por Vicente Ráo nos seguintes termos: "O fato, assim considerado, determina, pois, uma relação jurídica entre os sujeitos que o praticam e o ordenamento jurídico, o qual assenhoreando-se desta relação, passa a disciplinar, de certo modo, a conduta dos sujeitos. Se um deles, em virtude desse fato, está em situação de "dever", isto se entende no sentido de "dever" submeter— se ao ordenamento jurídico, a fim de observar, perante o outro sujeito, a conduta que este ordenamento lhe impõe. E se o outro se acha em situação de "poder", entende-se que o ordenamento jurídico lhe permite manter uma conduta correspondente à sua situação. Mas nem o "dever" significa uma submissão do primeiro sujeito ao segundo, nem o "poder" equivale a uma atribuição de força, ou comando, porventura pertencente ao segundo sobre o primeiro. Constituem os primeiros termos da relação, portanto, de um lado

Ainda em destaque na doutrina alemã, encontra-se, no pensamento de Karl Larenz, a visão tipológica dos direitos subjetivos, sobre os tipos tutelados, sua criação e as suas repercussões nas relações jurídicas:

> O tipo como forma de pensamento serve também à ciência do Direito para uma caracterização mais pormenorizada de certas espécies de relações jurídicas, em especial de direitos subjetivos e relações contratuais obrigacionais. […] Com «tipos» de direitos subjectivos alude-se aqui antes a tipos como direitos de personalidade, direitos de senhorio, direitos potestativos, direitos de cooperação e expectativas jurídicas, que não podem definir-se em sentido estrito. […]
> Os tipos de relações jurídicas, em especial os tipos contratuais, são tipos jurídicos-estruturais surgidos na realidade jurídica, que se referem à estrutura particular de cada uma das criações jurídicas. É assim que eu os denomino. Alguns deles, como os dos direitos subjectivos, são produtos da ciência do Direito; a maior parte deles, tais como todos os tipos de contratos obrigacionais, devem o seu surgimento ao tráfego jurídico. O legislador regulamentou-os, porquanto os encontrou previamente na realidade da vida jurídica, apreendeu-os na sua tipicidade e adicionou-lhes as regras que considerou adequadas para um tal tipo de contrato. Não os «inventou», mas «descobriu-os», porquanto não os tomou simplesmente da tradição jurídica. Mesmo no último caso, poderiam ter surgido originariamente na vida jurídica. O legislador não precisa, bem entendido, de assumir o tipo precisamente tal como se formou na vida jurídica; pode, mediante a sua regulamentação, introduzir-lhe novos traços e descurar outros.[124]

Assim, essas relações jurídicas de Direito Digital serão tanto relações previstas pelo legislador, como, por exemplo, um contrato de provisão de internet, nos termos previstos pelo MCI, como também uma infinidade de novas relações contratuais e consumeristas, até então desconhecidas, e que serão "descobertas" pelos juristas e pelo legislador na vida prática jurídica, como, por exemplo, os contratos de transporte individual de passageiros, via aplicativos de celulares.

---

o ordenamento jurídico e de outro os sujeitos ativos e passivos. A relação, porém, oriunda desses dois termos, refere-se, necessariamente, a alguma coisa, que lhe confere interesse. Esse quid, entre os dois primeiros termos, é constituído pelo objeto da relação; e, considerada do ponto de vista de sua atinência com este objeto, a relação consiste na necessidade, ou faculdade, de se observar um determinado comportamento disciplinado pela norma jurídica. Assim, três elementos estruturais já se configuram, subordinados ao ordenamento jurídico: a) os sujeitos; b) o objeto; c) o comportamento determinado pela norma. Contudo, esses elementos estruturais apenas conceituam uma idéia, um tipo, definido pelo ordenamento jurídico; não formam, ainda, uma realidade concreta. Deles advêm a propriedade, o usufruto, o crédito, e não minha propriedade, meu usufruto, meu crédito. Para que esses esquemas, esse tipos definidos abstratamente pelos códigos e pelas leis, se traduzam em realidade, ainda falta alguma coisa, falta um outro quid, tal o ato ou fato que, por sua aptidão para produzir uma relação jurídica concreta com referência a determinados sujeitos, recebe o nome de ato ou fato jurídico.". (RÁO, Vicente, O direito e a vida dos direitos. 6 ed. anot. atual. por Ovídio Rocha Sandoval. São Paulo: RT, 2004. p. 824).

[124] LARENZ, Karl. Metodologia da ciência do direito. Tradução José Lamego.6. ed. Lisboa: Fundação Calouste Gulbenkian, 2012. p. 662-663. Sobre os direitos subjetivos, ele ainda leciona: "Se na linguagem que se refere o domínio dos factos se define direito subjectivo, seja como «poder de vontade», como «relação de poder juridicamente regulada» ou como «interesse juridicamente protegido», está-se desse modo a assinalar o seu efeito na esfera social.". (LARENZ, Karl. Metodologia da ciência do direito. Tradução José Lamego. 6. ed. Lisboa: Fundação Calouste Gulbenkian, 2012. p. 275-276).

Essas relações jurídicas têm como objeto, isto é, como bem jurídico de interesse e de tutela, os dados tratados, com interesses não necessariamente e/ou unicamente econômicos, tanto individuais como difusos.[125] Quanto aos dados pessoais tratados, no sentido atribuído pela LGPD, esses são os dados de titularidade uma pessoa natural.[126]

O Direito Digital ainda encontra âmbito de aplicação para dados que não tenham uma titularidade imediatamente definida, mas que estejam inseridos no contexto de alguma relação jurídica.[127] Pense-se, por exemplo, nos dados públicos, de interesse da coletividade, e de tratamento pelo Estado, como, por exemplo, os dados relativos à vacinação de brasileiros e de estrangeiros residentes, durante a pandemia da COVID-19. Esses são dados de interesses difusos que também merecem tutela jurídica, sobretudo no que diz respeito à sua transparência, com o acesso público assegurado, também merecendo tutela quanto à garantia de sua qualidade, sendo dever da Administração Pública garantir a sua integridade.[128]

Conclusão

Sendo o ordenamento jurídico brasileiro o âmbito de pesquisa do presente estudo, é possível afirmar que o Direito Digital, enquanto ramo do Direito, é uma realidade reconhecida por expressiva parte da doutrina jurídica nacional, com produção na literatura especializada, conforme as referências bibliográficas indicadas. No campo acadêmico, o Direito Digital foi reconhecido formalmente pelo MEC como disciplina regular dos cursos de graduação em Direito, devendo fazer parte da formação técnico-jurídica no Brasil.

Tema controverso, contudo, diz respeito à autonomia científica do Direito Digital, tema que este texto não se ocupou, mas que foi objeto de pesquisa da tese de doutoramento da qual este se originou. A importância desse tipo de abordagem decorre dos inúmeros desafios que as TICs vêm impondo ao Direito, sobretudo aos direitos fundamentais e à dignidade da pessoa humana, tanto no ordenamento jurídico brasileiro, como também noutros países.

---

[125] Sobre os dados pessoais sendo tratados como mercadoria e a sua monetização, inclusive com demonstrações ilustrativas por diagramas, veja-se: LIMA, Daniela Cenci. O valor dos dados: breves considerações sobre monetização, controle e proteção. Revista de Direito e as Novas Tecnologias. São Paulo: RT. v. 11/2021. Abr.-Jun. 2021. Sobre o aspecto de ativo intangível das bases de dados de direitos autorais e uma possível tensão entre esses direitos e a comercialização de dados pessoais, veja-se: VIDAL, Carisia Baldoti Salles; QUINELATO, Pietra Daneluzzi. O valor patrimonial do dado pessoal em base de dados tutelada por direito autoral. Ius Gentium. v. 10. n. 1. p. 126-144. Jan.-Abr. 2019.

[126] LGPD (Lei nº 13.709/2018). Artigo 5º Para os fins desta Lei, considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

[127] Sobre "dados não pessoais", veja-se: GALIANO, Angelo [et al.]. I dati non personali: la natura e il valore. In: Rivista Italiana di Informatica e Diritto. Ano 2. f. 1, Florença. Março 2020. p. 61-77. Ainda sobre o tema veja-se também HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022. p. 99-103.

[128] Comunga-se com o entendimento manifesto por Wolfgang Hoffmann-Riem no sentido de que a proteção conferida pelo Direito não pode se limitar à proteção de dados individuais e pessoais, no que ele faz a seguinte advertência: "A necessidade de ajudar a moldar futuros desenvolvimentos por meio da lei afeta basicamente todos os usos possíveis das tecnologias digitais.". (HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022. p. 6.).

Com o advento das TICs, a partir do final do século XX, especialmente com a internet, a humanidade vem vivenciando importantes mudanças, muitas delas disruptivas, na cultura, no trabalho, na economia, nas artes e no Direito. Desse novo *modus vivendi*, também chamado de "digitalização da vida", ligado à computação ubíqua, surgem problemas concretos, inquietudes individuais e coletivas, que colocam em perigo real o respeito aos direitos fundamentais e à dignidade da pessoa humana, que passa a ser assediada numa nova dimensão de reificação, aquela decorrente do tratamento ilícito dos dados pessoais.

Diante desse ambiente, entende-se que a Ciência Jurídica atualmente necessita de uma abordagem sistêmica própria para atender às demandas decorrentes das relações e dos conflitos entre direitos subjetivos e a utilização das TICs, com a consolidação e o aprofundamento numa disciplina jurídica autônoma do ponto de vista científico, disciplina essa denominada Direito Digital.

O Direito Digital, enquanto disciplina jurídica específica e autônoma, é aquele ramo do Direito que estuda as relações jurídicas cujo objeto seja o tratamento de dados com a utilização das TICs, especialmente com o uso dos meios digitais. Essas relações jurídicas têm como objeto, isto é, como bem jurídico de interesse e de tutela, os dados tratados, com interesses não necessariamente e/ou unicamente econômicos, tanto individuais, como difusos.

Em relação à denominação Direito Digital, justifica-se a sua escolha em razão de ser a mais usal e da sua ampla acolhida pela doutrina brasileira, com a ressalva de que a expressão Direito das Tecnologias da Informação e Comunicação (DTIC) também poderia representar o mesmo fenômeno, a qual não se acolhe apenas por não ser de uso corrente na literatura jurídica brasileira atualmente. As TICs são o resultado da convergência entre as tecnologias da informação, as telecomunicações e a atividade de processamento de dados numa única tecnologia, especialmente no formato digital, abarcando neste conceito tanto tecnologias atuais como futuras.

Na gênese do Direito Digital está a bipartição entre a Informática Jurídica e o Direito da Informática. A Informática Jurídica nasce do primeiro contato dos juristas com a informática e consiste em métodos de utilização prática dos meios informáticos pelos operadores do Direito, sendo esses meios utilizados como um instrumento de trabalho no âmbito jurídico. O Direito da Informática nasce como a disciplina em que informática é tratada como objeto do Direito e, com advento da internet e das TICs, se desdobra, no ordenamento jurídico brasileiro, com uma sistematização própria, numa disciplina jurídica autônoma, denominada Direito Digital.

Destaque-se, finalmente, que autonomia disciplinar não é sinônimo de isolamento científico, nem de isolamento acadêmico, possuindo o Direito Digital marcado caráter multidisciplinar. A transversalidade e a multidisciplinaridade são características do Direito Digital, constituindo-se esse num ramo do Direito Misto, isto é, um ramo relacionável tanto ao Direito Público como ao Direito Privado, contando com produção doutrinária própria na literatura jurídica brasileira.

Referências bibliográficas

BITTENCOURT, Sidney. **Licitação de tecnologia da informação**: contratações de bens e serviços de informática e automação. Leme: J. H. Mizuno, 2015.

BRASIL. Ministério da Educação. Conselho Nacional de Educação. Câmara de Educação Superior. **Resolução nº 2**, de 19 de abril de 2021.Republicada no Diário Oficial da União de 20 abr. 2021.

CERQUEIRA, Tarcisio Queiroz. **Software**: lei, comércio, contratos e serviços de informática: manual de utilização para empresários de software e serviços, profissionais de informática e advogados. Rio de Janeiro: Esplanada, 2000.

DE LUCCA, Newton. Títulos e contratos eletrônicos: o advento da informática e suas consequências para a pesquisa jurídica. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coord.). **Direito & internet**: aspectos jurídicos relevantes. 2 ed. São Paulo: Quartier Latin, 2005.

DENNY, Danielle M. T. **Internet legal**. Piracicaba: Imagens DD, 2016. Disponível em: <https://docero.com.br/doc/xve8c1s>. Acesso em 03 dez. 2021.

GALIANO, Angelo [et al.]. I dati non personali: la natura e il valore. **Rivista Italiana di Informatica e Diritto**. Ano 2. f. 1, Florença. Março 2020. p. 61-77.

GRABOWSKI, Mark; ROBINSON, Eric P. **Cyber law and ethics**: regulation of the connected world. New York: Routledge, 2021.

GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini (Colab.). **Teoria da ciência jurídica**. 2 ed. São Paulo: Saraiva, 2009

HENDERSON, M.; GALLINA, J.; BRETT, M. Methods for accelerating geospatial data processing using quantum computers. **Quantum Machine Intelligence,** v. 3, n. 4, 2021.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. Rio de Janeiro: Forense, 2021.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução Italo Fuhrmann. 2 ed. Rio de Janeiro: Forense, 2022.

KU, Raymond S. R. **Cyberspace law**: cases and materials. New York: Wolters Kluwer, 2016.

LARENZ, Karl. **Metodologia da ciência do direito**. Tradução José Lamego. 6. ed. Lisboa: Fundação Calouste Gulbenkian, 2012.

LEMOS, Ronaldo; DI FELICE, Massimo. A vida em rede. Campinas: Papirus 7 Mares, 2014

LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Thomson Reuters, 2019.

LIMA, Daniela Cenci. O valor dos dados: breves considerações sobre monetização, controle e proteção. **Revista de Direito e as Novas Tecnologias**. São Paulo: RT. v. 11/2021. Abr.-Jun. 2021.

LLOYD, Ian J. **Information technology law**. 6 ed. Oxford: Oxford University, 2011.

LOPES, Alan Moreira; SANTOS, Keila; TEIXEIRA, Tarcisio. **Direito digital**: teoria e prática. São Paulo: Tirant lo Blanch, 2021.

LORENZETTI, Ricardo L. **Comércio eletrônico**. Trad. Fabiano Menke, notas Cláudia Lima Marques. São Paulo: RT, 2004.

LOSANO. Mario G. A informática jurídica vinte anos depois. **Revista dos Tribunais**, São Paulo, v. 715, p. 350-367, maio 1995.

LOSANO. Mario G. *A lei alemã de proteção de dados*. **Revista da Procuradoria-geral do Estado,** Porto Alegre, v. 11, n. 19, p. 11-22, 1981.

LOSANO. Mario G. *Lexicografia computacional e informática jurídica*. **Revista da Procuradoria-Geral do Estado,** Porto Aelgre, v. 10, n. 26, p. 67-71, 1980.

LOSANO, Mario G. **Lições de informática jurídica**. São Paulo: Resenha Tributária, 1974.

MACHADO, Fernanda de Vargas; COLOMBO, Cristiano. Inteligência artificial aplicada à atividade jurisdicional: desafios e perspectivas para sua implementação no Judiciário. **Revista da Escola Judicial do TRT 4**. Porto Alegre, v. 3. n. 5. p. 117-141, jan./jun. 2021.

MARTINS, A. G.; MARQUES, J. A. Garcia; DIAS, Pedro Simões. **Cyberlaw em Portugal**: o direito das tecnologias da informação e comunicação. Lisboa: Centro Atlântico, 2004.

McMAHON, David. **Quantum computing explained**. New Jersey: John Wiley, 2008.

MESSORI, Giulio. Legal tech. *In:* ZICCARDI, Giovanni; PERRI, Pierluigi (org.). **Dizionario legal tech**. Milano: Giuffrè Francis Lefebvure, 2020. p. 584-585.

NOVO, Benigno Núñez. Direito virtual. **Boletim Jurídico**, v. 19, n. 1028, ago. 2019. Disponível em: <https://www.boletimjuridico.com.br/artigos/direito-e-internet/4484/direito-virtual>. Acesso em: 28 abr. 2021.

NUNES, Dierle; DUARTE, Fernanda Amaral. Jurimetria e tecnologia: diálogos essenciais com o direito processual. **Revista de Processo**. v. 299. São Paulo: RT Jan. 2020. p. 405-448.

NUNES, Marcelo Guedes. **Jurimetria**: como a estatística pode reinventar o direito. 2 ed. São Paulo: RT, 2019.

NUNES, Marcelo Guedes. O que é jurimetria? **Revista de Direito Bancário e do Mercado de Capitais**. v. 62. p.253-260. Out. - Dez. 2013.

PAESANI, Liliana Minardi. **Direito de informática**: comercialização e desenvolvimento internacional do software. 6. ed. atual. São Paulo: Atlas, 2009.

PAESANI, Liliana Minardi. **Direito de informática**: comercialização e desenvolvimento internacional do software. 10. ed. São Paulo: Atlas, 2015.

PANDETTISTICA. *In:* ENCICLOPEDIA del diritto. Milão: Garzanti. 2001.

PECK, Patricia. **Direito digital**. São Paulo: Saraiva, 2002.

PELLEGRINI, François; CANEVET, Sébastien. Le droit du numérique: une histoire à préserver. Vers un Musée de l'Informatique et de la Société Numérique en France. **Conservatoire National des Arts et Métiers**, Nov. 2012, Paris, France. pp.61-76. Disponível em <hal.inria.fr/hal.-00768912>. Acesso em 04 dez. 2021.

PINHEIRO, Patrícia. Peck. **Direito Digital**. 7 ed. rev. ampl. atual. São Paulo: Saraiva, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 06 nov. 2021.

RÁO, Vicente, **O direito e a vida dos direitos**. 6 ed. anot. atual. por Ovídio Rocha Sandoval. São Paulo: RT, 2004.

REALE, Miguel. **Lições preliminares de direto**. 21. ed. rev. atual. ampl. São Paulo: Saraiva, 1994.

REED, Chris. **Internet law**: text and materials. 2. ed. Cambridge: Cambridge University Press, 2004.

REZENDE, Denis Alcides. A evolução da tecnologia da informação nos últimos 45 anos. **Revista FAE BUSINESS**, Curitiba, n. 4. dez. 2002. Disponível em: <https://img.fae.edu/galeria/getImage/1/16578659447373246.pdf>. Acesso em: 28 abr. 2021.

RUFFOLO, Ugo (Org). XXVI Lezioni di Diritto dell'Intelligenza Artificiale. Turim: Giappichelli, 2021.

SIQUEIRA JÚNIOR, Paulo Hamilton. Direitos humanos e cidadania digital. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). **Direito & Internet**

III. São Paulo: Quartier Latin, 2015. v. 1: Marco Civil da Internet (Lei n. 12.965/2014). p. 171-185.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 3. ed. atual. ampl. São Paulo: Saraiva, 2015.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

VIDAL, Carisia Baldoti Salles; QUINELATO, Pietra Daneluzzi. O valor patrimonial do dado pessoal em base de dados tutelada por direito autoral. **Ius Gentium**. v. 10. n. 1. p. 126-144. Jan.-Abr. 2019.

ZICCARDI, Giovanni. **Manuale breve:** informatica giuridica. Milano: Giuffrè, 2006.

ZICCARDI, Giovanni. Informatica giuridica. *In:* ZICCARDI, Giovanni; PERRI, Pierluigi (org.). **Dizionario legal tech**. Milano: Giuffrè Francis Lefebvure, 2020. p. 520.

Vale mais uma imagem do que mil palavras? O mal-uso de deep fakes e a sua regulamentação no Direito brasileiro

Sylvia Chaves da Silva Ramos[129]

RESUMO

Em termos de avanço no campo da Inteligência Artificial, a sociedade tem experimentado uma significativa melhora na qualidade de vida, conforto, bem como maior acessibilidade e estreitamento de relações. Por outro lado, surgem desafios, que, na mesma proporção daqueles benefícios, são extremamente desenvolvidos, sofisticados e, por consequência, de difícil solução. Um deles, advindo da Sociedade 4.0, é a rápida propagação de deep fake, espécie do gênero fake news, empre cada vez mais para fins espúrios, desde pornografia de vingança até desequilíbrio no pleito eleitoral via propaganda eleitoral negativa criminosa. E é sobre o impacto dos vídeos e imagens fraudados para fins eleitoralistas que o presente artigo irá abordar.

PALAVRAS-CHAVE

Inteligência artificial; Machine Learning; Deep fake; Fake News; Direito Eleitoral.

[129] Professora da Universidade Estácio de Sá e Advogada. Doutora em Direito pela Universidade do Estado do Rio de Janeiro (UERJ).

A picture is worth a thousand words? The misuse of deep fakes and their regularization in Brazilian law

Sylvia Chaves da Silva Ramos

ABSTRACT

In terms of advancement in the field of Artificial Intelligence, society has experienced significant improvement in quality of life, comfort, greater accessibility, narrowing of relationships. On the other hand, challenges arise, which, in the same proportion as those benefits, are extremely developed, sophisticated and, consequently, difficult to solve. One of these, arising from Society 4.0, is the rapid propagation of deep fake, a species of the fake news genre, increasingly used for spurious purposes, from revenge pornography to electoral imbalance via criminal negative electoral propaganda. And it is on the impact of fraudulent videos and images for electoral purposes that this article will address.

KEYWORDS

Artificial Intelligence; Machine Learning; Deep fake; Fake News; Electoral Law.

"Generative Adversarial Networks is the most interesting
idea in the last ten years in machine learning"

LECUN, Yann
Vice-Presidente e Cientista-Chefe
de Inteligência Artificial do Facebook

Introdução

Machine learning, algoritmos, inteligência artificial, *deep learning*, têm sido algumas das expressões comumente utilizadas nas profissões de Tecnologia da Informação, mas que vêm ocupando o vocabulário de boa parte das pessoas ao redor do mundo. Tal fenômeno ocorre porque, sobretudo a partir de 2015, a Inteligência Artificial passa a ser aplicada a todos os campos e áreas de conhecimento. O uso das técnicas de aprendizado de máquina aliado à comunicação, marketing e entretenimento digital não geram dúvidas de que a IA está entranhada em nosso cotidiano.[130]

Todo o avanço tecnológico gera benefícios e, juntamente com eles, algumas mazelas a serem enfrentadas no seio social. A distância entre pessoas foi encurtada e o espaço público para debate de ideias, por outro lado, fora ampliado[131]. Como consequência dessas transformações, ocorre a propagação da desinformação pelas notícias falsas, de um modo alarmante e de difícil contenção.

No presente, o ambiente virtual é palco das mais variadas modalidades de crimes contra a honra, cometidas por meios de divulgação em massa via mídias sociais, tais como *Instagram*, *TikTok*, *Facebook*. Essas informações fraudulentas estão destruindo a boa imagem que uma pessoa tem ou que almeja construir.

Nesse contexto, as *fake news* assumem um espectro mais sofisticado, repleto de artifícios tecnológicos, que dificultam ainda mais a identificação daquilo que vem a ser verdadeiro ou falso. Em verdade, podem ser definidas como mentiras qualificadas "pelo dolo e pelo dano".[132]

---

[130] LAGE, Fernanda de Carvalho. *Manual de Inteligência Artificial no Direito Brasileiro*. Salvador: Editora JusPodivm, 2021. P.35.

[131] À essa ampliação do espaço público para o debate de ideias, Castells analisa a ascensão da "*noopolitik*", termo proposto pelos estudiosos Arquilla e Ronfeld. "A '*noopolitik*' diz respeito às questões políticas que surgem da formação de uma "noosfera", ou ambiente de informação global, que inclui o ciberespaço e todos os outros sistemas de informação – a mídia, por exemplo. A *noopolitik* pode ser contraposta à *realpolitik*, a abordagem tradicional em termos de promoção do Estado na arena internacional, mediante negociação, força ou uso potencial de força. A *realpolitik* não desaparece na Era da Informação. Mas permanece centrada no Estado, numa era organizada em torno de redes, inclusive redes de Estados. Num mundo caracterizado por interdependência global e moldado pela informação e a comunicação, a capacidade de atuar sobre fluxos de informação, e sobre mensagens da mídia, torna-se uma ferramenta essencial para a programação de um programa político". CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade, Maria Luiza X. de A. Borges* (trad.) Rio de Janeiro: Jorge Zahar Ed., 2003. P. 132.

[132] RAIS, Diogo. *Seminário Internacional Fake News e Eleições [recurso eletrônico]: anais*. Brasília: Tribunal Superior Eleitoral, 2019. P. 36. Disponível em: <https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/5981/2019_seminario_fake_news_eleicoes.pdf?sequence=8&isAllowed=y> Acesso: 8 de maio de 2022.

A boa doutrina classifica as notícias fraudulentas quanto a tecnologia informacional empregada.[133] No primeiro grupo, encontram-se as chamadas *shallow fakes*, isto é, edição de vídeos com arquivos descontextualizados, mas sem a alteração do seu teor. Nesse tipo manipulação, a qualidade do material final é grosseira, facilmente perceptível pelo homem médio, sem conhecimentos refinados de programação.

Como segundo grupo, há as *deep fakes*, muitos mais persuasivas e de fácil convencimento de seu expectador. São rotineiramente utilizadas como arma publicitária contra rivais políticos em pleitos eleitorais. E é exatamente sob esse contexto que o presente trabalho se concentrará.

1. O que são as *Deep-Fakes*?

Deep fakes são informações inverídicas elaboradas através da contribuição da inteligência artificial. Sob o manto do aprendizado profundo[134], o agente manipula vídeos, imagens e áudios inserindo conteúdos falsos, consoante os objetivos almejados. Daí, surge a expressão fruto da combinação das palavras *deep* = *deep learnig*, e *fake* = algo falso, manipulado.[135]

Há diversas maneiras de criar uma *deep fake*. Uma das mais adotadas se vale do emprego de Redes Geradoras Adversariais (GAN), composta por duas redes neurais profundas, uma chamada gerador e a outra, discriminador. A primeira gera os dados, enquanto que a segunda treina o uso de dados, buscando a verdade. A *deep fake* só estará apta a produzir seus efeitos quando o discriminador não conseguir mais distinguir se o conteúdo é verdadeiro ou falso.

Para fins didáticos, vale apresentar o detalhamento do processo, cuidadosamente descrito por Michael Filimowicz

> The creation of deep fake videos requires a large dataset of publicly available video footage and audios files, then employing deep learning by machines teaching themselves as machine learning models. Deep fakes are made possible by two neural networks known as generative adversarial networks (GAN) working together as the "generator" and the "discriminator". The first machine learning processo, the generator, involves training on a dataset composed of a large swathe of images drawn from publicly available sites that enables it to learn and mimic a person's facial expressions and voice. The harvested images center on a target subject that includes as many face and body angles with features and expressions under multiple lighting conditions. Video forgeries are created from data collected in this first stage of the process after swapping it onto another person by employing a deep learning algorithm. Once a vídeo forgery has been made, its creators manually fine tune some of the resultads to avoid obvious image problems like glitches. The second machine learning model, the discriminator, ins then employed to detect those forgerires is the deep fake complete.[136]

---

[133] MENEZES, Paulo Brasil. *Fake News: modernidade, metodologia e regulação*. Salvador: Editora JusPodivm, 2021. P. 117.

[134] *Deep learning* é "um subdomínio do aprendizado de máquina, que consiste em múltiplas camadas em cascata, modeladas a partir do sistema nervoso humano (uma prática denominada codificação neural), conhecida como rede neural articular. Arquiteturas de aprendizagem profunda permitem que um sistema de computador se treine usando dados históricos, reconhecendo padrões e fazendo inferências probabilísticas". LAGE, Fernanda de Carvalho. *Op. Cit*., p. 70.

[135] "[...] a combination of 'deep learning' and 'fake, deep fakes are hyper-realistic videos digitally manipulated to depict people saying and doing things that never actually happened". WESTERLUND, Mika. The emergence of deep fake technology: a review. *In: Technology Innovation Management Review. v. 9, nº 11, nov. 2019*. Disponível em: <https://timreview.ca/article/1282> Acesso em: 7 de maio de 2022.

[136] FILIMOWICZ, Michael. *Deep fakes: algorithms and Society*. Nova Iorque: Routledge Focus, 2022. P. 1997-1998.

Não se nega que as *deep fakes* têm sido empregadas para fins legítimos, como no cinema, nos videogames, nos clipes musicais, criando até mesmo uma experiência de realidade virtual em museus e mídias educativas. À título de exemplo, no ano de 2019, o Museu Dalí, localizado em São Petersburgo, Flórida, utilizou a tecnologia *deep fake* para "ressucitar" Salvador Dalí (1904-1989) e fazer a atração interagir com seus convidados, resultando em boas selfies e muitas risadas.

Infelizmente, a adoção dessa ferramenta poderosa é muito frequente entre políticos para descredibilizar seus adversários e influenciar no resultado dos processos eleitorais.

Um caso conhecido no Brasil envolveu João Doria, Governador de São Paulo, inclusive candidato à Presidência na eleição que se avizinha. Durante o pleito de 2018, circularam nas redes sociais um vídeo de sexo explícito entre seis mulheres e um homem, supostamente Doria.[137]

Outro episódio, que gerou repercussão à nível internacional, ocorreu com a divulgação de um vídeo, veiculado no YouTube, em que Barack Obama teria dito que "o Presidente Trump é um total e completo imbecil". O rosto, a voz e os movimentos pareciam ser de Obama, porém, tratava-se de conteúdo digital manipulado.

Episódios como os acima narrados vêm despertando maior preocupação do Tribunal Superior Eleitoral sobre a matéria, ao ponto de, periodicamente, a Corte realizar estudos e eventos sobre a matéria.[138]

Não há dúvidas de que *deep fakes*, se bem formatadas, têm o condão de gerar imagens e/ou vozes extremamente parecidas com a realidade, hábeis a convencer o público quase que instantaneamente.[139]

De acordo com pesquisa apresentada por Maurício Moura, em 2019, durante o Seminário Internacional entre estudiosos brasileiros e europeus, organizado pelo TSE, somente no mês de maio daquele ano houve um incremento de 67% de divulgações de notícias falsas em todo o Brasil. Acrescenta o investigador que "a *fake news* perpassa todas as campanhas eleitorais de maneira muito forte. Outro dado que é comum aos Estados Unidos, à Índia, ao Brasil, à Espanha: as pessoas confiam mais no conteúdo recebido por familiares e amigos do que no conteúdo da imprensa tradicional".[140]

Nesse diapasão, Citron e Chesney apresentam três grandes fenômenos que geram a viralização das *deep fakes*. O primeiro deles é a falta de atenção das pessoas para assimilar informações fidedignas, ou, nas palavras dos autores, a "dinâmica da informação em cascata". A maioria delas não colocariam suficiente atenção às notícias que lhes

---

[137] Até a data de fechamento desse artigo, não houve perícia do material em juízo, atestando veracidade ou manipulação do conteúdo do vídeo.

[138] No Brasil, o Tribunal Superior Eleitoral (TSE) é responsável pela edição de Resoluções que, além de tornar o processo eleitoral mais seguro e previsível, dão suporte à toda a jurisdição eleitoral.

[139] LEAL, Luziane de Figueiredo Simão. Inteligência Artificial nas campanhas eleitorais: a democracia das plataformas no banco dos réus. Belo Horizonte: Dialética, 2020. P. 72-73.

[140] MOURA, Maurício. *Seminário Internacional Fake News e Eleições [recurso eletrônico]: anais*. Brasília: Tribunal Superior Eleitoral, 2019. 58. Acesso em: 2 de maio de 2022. https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/5981/2019_seminario_fake_news_eleicoes.pdf?sequence=8&isAllowed=y

são apresentadas, acreditando em tudo que escutam ou ouvem sem, contudo, questionar. O segundo fato se concentra na tendência de compartilhamento de informações negativas e novas, em tom de "fofoca", o que, supostamente, seria um conteúdo mais interessante à vista do receptor. Por fim, outro fator que corrobora com a divulgação massiva dessas informações falsas é o algoritmo através dos denominados "filtros de bolhas", que capta os conteúdos mais divulgados na rede e propaga para os demais *leads* com interesses semelhantes.[141]

Em tempos de conquistas de espaço e poder, a tecnologia da informação vem sendo um verdadeiro mecanismo de involução do processo democrático. Adversários políticos e grandes players econômicos aliados a estes, e ao mesmo tempo entrelaçado com a gestão pública, assim como a própria sociedade moderna, se valem de notícias falsas para impactar as votações, e, consequentemente, causar desordem para o ambiente institucional e social das democracias globais.

À tais manifestações têm-se conferido uma nova roupagem à velha política, na medida em que as *deep fakes* são empregadas "em um meio que permite uma veloz massificação dos discursos de tal forma que coloca em risco a credibilidade do espaço e da informação que nele circula".[142]

> Com efeito, faz-se importante ressaltar que é no período eleitoral, durante as propagandas políticas, que o uso de *bots* pode colocar em xeque a higidez do processo democrático de escolha de candidatos políticos porque é nessa época que a massificação do uso de *fake news* adquire contornos de propaganda política pró ou contra candidatos, potencializando a influência no resultado da votação.[143]

De fato, consoante os ensinamentos de José Jairo Gomes, os objetivos da propaganda eleitoral não são outros senão influir na vontade do eleitor e obter a vitória no certame.[144] Contudo, anda na contramão da dimensão coletiva da liberdade de expressão, conteúdos que tenham o condão de prejudicar outrem, como, por exemplo, a propaganda eleitoral negativa criminosa, quando adversários políticos e/ou aliados divulga fatos inverídicos ou caluniosos com o fito de desqualificar a pessoa do candidato, sugerindo que esta "não detém os adornos morais ou a aptidão necessária à investidura em cargo eletivo".[145]

Nesse contexto, o cidadão é inserido em uma dicotomia, onde, de um lado estão as mídias sociais, que ampliam o espaço democrático de debates legítimos de ideias, e,

---

[141] CHESNEY, Bobby; CITRON, Danielle. Deep Fakes: A Looming Challenge for Privacy, Democracy, and national Security. *In: California Law Review 1753* (2019), p. 1765-1768. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954> Acesso: 8 de maio de 2022.

[142] RUEDIGER, Marco Aurélio (coord.). *Bots e o Direito Eleitoral brasileiro nas eleições de 2018 [Policy Paper]*. Rio de Janeiro: FGV DAPP, 2018. P. 5. Disponível em: <http://twixar.me/DmNT>. Acesso em: 7 maio de 2022.

[143] DIAS, Jefferson Aparecido; SILVA, Fabiano Fernando da. Bots, fake news, fake faces, deep fakes e sua eventual influência no processo eleitoral democrático. *In: Revista da Advocacia do Poder Legislativo, v. 2, ano 2021*, p. 39.

[144] GOMES, José Jairo. Direito Eleitoral, 14ª. ed. rev., atual. e ampl. (e-book). São Paulo: Atlas, 2018. P. 500.

[145] *Idem*, p. 279.

de outro, a forte disseminação de inverdades por agentes maliciosos, com vista a dominar fraudulentamente o cenário político.

Para que haja um processo eleitoral democrático, é imprescindível que a formação do convencimento do eleitor seja livre, isenta de quaisquer tipos de manipulações. E é por esse motivo, que a Justiça Eleitoral e o Poder Legislativo devem adotar medidas profiláticas no sentido de assegurar que as redes sociais serão utilizadas como instrumento diálogo legítimo, de participação popular, liberto do impacto negativo da desinformação, tão recorrente com o advento das rápidas transformações tecnológicas.[146]

2. Panorama Legislativo Brasileiro atual de combate à Desinformação

As *deep fakes* são comumente empregadas, ao redor do globo, para influenciar o processo democrático eleitoral, através do bombardeamento de informações falsas. Entretanto, em que pese o impacto negativo desses mecanismos sofisticados de desinformação, a realidade é que no Brasil, não há lei específica que regule a matéria.

Diante dessa lacuna normativa, é imperioso que o operador do direito se valha ao menos de alguns parâmetros legais para o enfrentamento dessa prática, podendo-se citar, por exemplo, o artigo 242, do Código Eleitoral. Consoante teor desse dispositivo, é vedado à propaganda eleitoral criar, artificialmente, na opinião pública, estados mentais, emocionais ou passionais.

Recentemente, com o advento da Lei n.º 14.192, de agosto de 2021, o Código Eleitoral, sofreu diversas alterações, dentre elas, a criminalização da divulgação de fato ou vídeo com conteúdo sabidamente inverídico no período de campanha eleitoral.[147]

Agregue-se a tais previsões o art. 27, §1°, da Resolução n.º 23.610/19, que, na esteira das disposições anteriores, coíbe a ofensa à honra ou imagem de candidatas, candidatos, partidos, federações ou coligações, bem como a divulgação de informações inverídicas.[148]

Segue em tramitação o Projeto de Lei nº 3.683/20, da relatoria do Senador Angelo Coronel, que visa inserir o § 3º, no art. 53, da Lei das Eleições (Lei n.º 9.504/97) para efetivamente tipificar as *deep fakes*. Consoante a redação originária do Projeto, "em caso de uso de conteúdo de áudio, vídeo ou imagem deliberadamente alterado ou fabricado

---

[146] DIAS, Jefferson Aparecido; SILVA, Fabiano Fernando da. Op. cit., p. 37.

[147] "Art. 323, do Código Eleitoral brasileiro. Divulgar, na propaganda eleitoral ou durante período de campanha eleitoral, fatos que sabe inverídicos em relação a partidos ou a candidatos e capazes de exercer influência perante o eleitorado: (Redação dada pela Lei nº 14.192, de 2021) Pena - detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa. Parágrafo único. Revogado. (Redação dada pela Lei nº 14.192, de 2021) § 1º Nas mesmas penas incorre quem produz, oferece ou vende vídeo com conteúdo inverídico acerca de partidos ou candidatos. [...]"

[148] Art. 27, da Resolução n.º 23.610/19. É permitida a propaganda eleitoral na internet a partir do dia 16 de agosto do ano da eleição (Lei nº 9.504/1997, art. 57- A). § 1º A livre manifestação do pensamento de pessoa eleitora identificada ou identificável na internet somente é passível de limitação quando ofender a honra ou a imagem de candidatas, candidatos, partidos, federações ou coligações, ou divulgar fatos sabidamente inverídicos, observado o disposto no art. 9º-A desta Resolução. [...]"

para imitar a realidade, com o objetivo de induzir a erro acerca da identidade de candidato a cargo público ou colocar em risco a credibilidade e a lisura das eleições, as sanções previstas no §1º serão aumentadas de 1/3".[149]

No corpo da Exposição de Motivos do PL n.º 3683/20, o parlamentar reconhece o potencial ofensivo dessa modalidade de *fake news*. Ressalta a total viabilidade de alteração de imagens, vídeos e voz de modo que, para a maioria das pessoas, seja quase impossível distinguir na montagem o que seja falso ou manipulado. Por essa razão, afirma que a referida conduta merece resposta dura, especialmente se o uso for na seara eleitoral, sobretudo porque "nesse espaço o que está em risco não é simplesmente a reputação de um candidato a cargo público, mas a própria percepção da sociedade sobre os representantes que ela precisa eleger. O potencial de fragilizar nossa democracia é gigantesco".[150]

O referido Projeto, no momento, encontra-se, desde dezembro de 2021, na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, aguardando a designação de Relator.

É bem verdade que o Tribunal Superior Eleitoral envida esforços contínuos na tentativa de combater as *fake News*. À título de exemplo, vale citar: 1) a criação do Conselho Consultivo sobre Internet e Eleições, através da Portaria nº 949, de 7 de dezembro de 2017, com o objetivo de "desenvolver pesquisas e estudos sobre as regras eleitorais e a influência da Internet nas eleições, em especial o risco das *fake news* e o uso de robôs na disseminação das informações" (art. 2º, I); 2) a realização do o Seminário Internacional *Fake News* e Eleições, em maio de 2019, em parceria com a delegação da União Europeia no Brasil; 3) a veiculação de vídeos educativos com o fim de explicar ao eleitorado o que vem a ser *deep fakes*, porém, tais medidas ainda se mostram deficitárias para atacar a onda massiva de divulgação de notícias falsas, sobretudo agora que houve mutação das *fake news* para formas mais avançadas, com uso de recursos tecnológicos mais inovadores.

Por óbvio, há diversas ferramentas de Inteligência Artificial que, se agregadas à regulamentação específica da matéria, serão muito bem-sucedidas no combate às notícias falsas. Aqui se está a falar do uso da mesma tecnologia para identificá-las, através de programas e apps de identificação de fraudes. Nesse sentido, destaca Westerlund,

> Technological solutions, including automated tools for deepfake detection, content authentication, and deepfake prevention constitute a dynamic field of security methods. It is quickly becoming impossible for human beings to distinguish between real and fake videos. Hence, our results list numerous cues for detecting deepfakes, and suggest harnessing AI in order to detect AI-generated fakes as an efficient combat strategy. Further, another emerging technology, namely blockhain can be of help. Blockchain technology is not only highly resistant to forgeries and can store

[149] BRASIL. Senado Federal. Projeto de Lei nº 3.683, de 07 de julho de 2020. Altera a legislação criminal, eleitoral e de improbidade administrativa para elevar penas e sanções de crimes já tipificados e outras condutas ilegais, e criar novos tipos penais, especialmente quando praticados na internet. Brasília: Senado federal, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8861739&ts=1644253833773&disposition=inline>. Acesso em: 08 maio de 2022.

[150] *Idem*, p. 9.

> data in an accruable, safe, transparent, and traceable way, but it can also track and certify the origins and history of the data.[151]

Ronaldo Lemos corrobora com a sugestão do uso de tais certificados de realidade, com base na tecnologia *blockchain*. "Se uma imagem sofre alguma alteração, perde então o 'certificado', indicando que pode ter sido manipulada. Essa solução é imperfeita. Nenhum fabricante está disposto a fazer isso até o momento". [152]

Maurício Moura alerta que a tecnologia só irá ampliar a complexidade da inteligência artificial, apenas agregará dificuldade aos fraudadores. Por esse motivo, sustenta que a verdadeira arma de combate às notícias falsas, "está na sala de aula, da educação básica até a universidade. Esse é o verdadeiro campo de batalha da *fake news*". [153]

É inegável que a educação e treinamento também são cruciais para o combate à *deep fakes*. Urge a necessidade de conscientização da sociedade sobre os riscos do uso indevido da Inteligência Artificial. Empresas, governo e órgãos regulamentadores precisam compreender a necessidade educação digital, com vistas a contribuir para a fomentação de senso crítico e, consequente, capacidade de identificação de *fake news* sobretudo no ambiente virtual.

Trata-se, em verdade, de um novo capítulo da história da humanidade em que é exigido da sociedade uma resposta incisiva, não limitada aos tradicionais tipos penais existentes no Código Penal de 1940 ou no Código Eleitoral de 1965, mas aliado a métodos profiláticos a serem cautelosamente delineados através de esforço conjunto da Administração Pública, Legislativo, organizações e Instituições de Ensino.

Conclusão

O presente trabalho teve por escopo a análise de um dos maiores desafios tecnológicos enfrentados pela sociedade contemporânea, o mal-uso das *deep fakes* nas campanhas eleitorais.

---

[151] WESTERLUND, Mika. *Op. cit*, p. 47.

[152] Contudo, a estratégia que realmente entusiasma o autor é a chamada certificação de álibi, através de autovigilância preventiva. A proposta recomenda a gravação de toda e qualquer palavra que que o indivíduo pronuncia, o registro de todos os lugares em que esteve, as pessoas que encontrou, ou seja, certificaria 100% da vida de uma pessoa. Daí, caso um agente malicioso venha a criar uma *deep fake* sobre a pessoa, a certificação de álibi seria capaz de afirmar, com base nos registros, que a vítima não falou a mensagem que constava no simulacro, não se encontrou terceiros que estavam na imagem e, tampouco, esteve no local. O próprio estudioso afirma se tratar de uma proposta de difícil aceitação. De fato, ninguém ousaria abrir mão de sua intimidade ao ponto de registrar cada ação, cada passo que realiza, porém, Lemos sustenta que "no mundo em que estamos vivendo hoje, não seria surpresa que pessoas públicas, como presidentes ou juízes das Supremas Cortes, adotassem esse tipo de estratégia como medida preventiva". LEMOS, Ronaldo. Como combater deepfakes? Folha de São Paulo, São Paulo, 11 de março de 2019. Coluna de Ronaldo Lemos na Folha de São Paulo. Disponível em: <https://itsrio.org/pt/artigos/como-combater-deepfakes/>. Acesso em: 10 de maio de 2022.

[153] MOURA, Maurício. Seminário Internacional Fake News e Eleições (2019: Brasília, DF). Seminário Internacional Fake News e Eleições [recurso eletrônico] anais. Brasília: Tribunal Superior Eleitoral, 2019. P. 64. Acesso em: https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/5981/2019_seminario_fake_news_eleicoes.pdf?sequence=8&isAllowed=y

De um lado, têm-se um espaço público de debate ampliado, para a apresentação e crítica de ideias político-partidárias, e de outro, a involução do processo democrático sob a forma de desinformação, via compartilhamento massivo de notícias falsas.

As *deep fakes*, modalidade altamente sofisticada de *fake news*, dado o uso do *machine learning* para sua criação, acabam por persuadir um sem número de indivíduos que dão crédito ao seu conteúdo, sem, contudo, questionar a fonte ou o material que lhe é apresentado. E, como visto em linhas anteriores, não é para menos. Com uma educação deficitária em matéria de uso consciente de tecnologia da informação, as pessoas atuam de acordo com a sua consciência, sem mensurar os riscos que um simples clique pode causar a reputação de outrem.

O Brasil ainda engatinha na regulamentação do emprego da Inteligência Artificial, pouco a pouco desenvolvendo estudos com Nações irmãs que possuem um ordenamento jurídico mais avançado, como é o caso de Portugal.

Entretanto, o legislador brasileiro, sobretudo em matéria eleitoral, entende que para que haja ferramentas jurídicas ou tecnológicas hábeis a combater *deep fakes* e os demais formatos de notícias fraudulentas, é indispensável a adequação de métodos já existentes em outros países à realidade de nosso cenário interno. A mera internalização de corpos normativos internacionais, sem maiores reflexões, acabará por gerar o fenômeno da americanização ou europeização do Direito, tão comum em outras áreas jurídicas.

E, a indagação inicial "vale mais uma imagem do que mil palavras?" talvez seja agora respondida com propriedade. Um ditado popular, aparentemente simples, até então tido como verdade absoluta, passa a assumir contornos profundos, deixando claro que, apesar do impacto que um vídeo, foto ou gravação de voz acarrete no inconsciente das pessoas, com a evolução e aprimoramento da Inteligência Artificial, merece ser questionado.

Como mencionado, está-se a redigir linhas de um novo capítulo da história da humanidade, cujo objeto não tem volta, apenas o avanço, o avanço do uso consciente da Inteligência Artificial.

Bibliografia

BRASIL. Senado Federal. Projeto de Lei nº 3.683, de 07 de julho de 2020. Altera a legislação criminal, eleitoral e de improbidade administrativa para elevar penas e sanções de crimes já tipificados e outras condutas ilegais, e criar novos tipos penais, especialmente quando praticados na internet. Brasília: Senado federal, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8861739&ts=1644253833773&disposition=inline>.

CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade, Maria Luiza X. de A. Borges (trad.) Rio de Janeiro: Jorge Zahar Ed., 2003.

CHESNEY, Bobby; CITRON, Danielle. Deep Fakes: A Looming Challenge for Privacy, Democracy, and national Security. *In: California Law Review 1753* (2019). Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954>.

DIAS, Jefferson Aparecido; SILVA, Fabiano Fernando da. Bots, fake news, fake faces, deep fakes e sua eventual influência no processo eleitoral democrático. *In: Revista da Advocacia do Poder Legislativo, v. 2, ano 2021*.

FILIMOWICZ, Michael. *Deep fakes: algorithms and Society*. Nova Iorque: Routledge Focus, 2022.

GOMES, José Jairo. Direito Eleitoral, 14ª. ed. rev., atual. e ampl. (e-book). São Paulo: Atlas, 2018.

WESTERLUND, Mika. The emergence of deep fake technology: a review. *In: Technology Innovation Management Review*. v. 9, nº 11, nov. 2019. Disponível em: <https://timreview.ca/article/1282>

LAGE, Fernanda de Carvalho. Manual de Inteligência Artificial no Direito Brasileiro. Salvador: Editora JusPodivm, 2021.

LEAL, Luziane de Figueiredo Simão. Inteligência Artificial nas campanhas eleitorais: a democracia das plataformas no banco dos réus. Belo Horizonte: Dialética, 2020.

LEMOS, Ronaldo. Como combater deepfakes? Folha de São Paulo, São Paulo, 11 de março de 2019. Coluna de Ronaldo Lemos na Folha de São Paulo. Disponível em: <https://itsrio.org/pt/artigos/como-combater-deepfakes/>.

MENEZES, Paulo Brasil. Fake News: modernidade, metodologia e regulação. Salvador: Editora JusPodivm, 2021.

RAIS, Diogo. Seminário Internacional Fake News e Eleições [recurso eletrônico]: anais. Brasília: Tribunal Superior Eleitoral, 2019.

RUEDIGER, Marco Aurélio (coord.). Bots e o Direito Eleitoral brasileiro nas eleições de 2018 [Policy Paper]. Rio de Janeiro: FGV DAPP, 2018. P. 5. Disponível em: <http://twixar.me/DmNT>.

TRIBUNAL SUPERIOR ELEITORAL. Seminário Internacional Fake News e Eleições [recurso eletrônico]: anais. Brasília: Tribunal Superior Eleitoral, 2019. Acesso em: 2 de maio de 2022. https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/5981/2019_seminario_fake_news_eleicoes.pdf?sequence=8&isAllowed=y

II_Outros Estudos

Os diferentes processos de consentimento na pesquisa envolvendo seres humanos e na assistência à saúde e a Lei de Proteção de Dados brasileira[154]

Márcia Santana Fernandes[155]
José Roberto Goldim[156]

RESUMO

A área da saúde envolve diferentes processos de consentimento, os quais têm natureza e finalidades distintas, assim como diferentes efeitos jurídicos. Neste texto são analisados as distinções e os pontos de conexão entre o processo de consentimento na área da saúde, na pesquisa clinica e na assistência à saúde, envolvendo adultos, crianças e adolescentes à luz da Lei Geral de Proteção de Dados brasileira - LGPD; Lei 13.709/2018. Este estudo está organizado em três Partes: a Parte I trata do processo de consentimento na pesquisa clínica (envolvendo seres humanos); na Parte II trata do processo de consentimento na assistência à saúde, em particular considerando a possibilidade de tratamento de dados pessoais no art. 7º e no art. 11 do LGPD, destacando em particular as semelhanças e diferenças entre as bases legais para o tratamento de dados pessoais e o consentimento manifestado no contexto da assistência à saúde e por fim, na Parte III, enfrenta-se o processo de consentimento envolvendo crianças e adolescentes em situações de pesquisa clínica e em assistência na área da saúde, assim como a sua relação com o previsto na LGPD. O método utilizado foi de revisão narrativa de literatura, com base em textos publicados nas línguas portuguesa, inglesa e espanhola. Como conclusão geral, cabe pontuar que o ato humano de consentir está diretamente conectado ao exercício da liberdade. O consentimento pode representar diferentes formas e sentidos de manifestação de vontade, tendo este ato efeitos jurídicos ou não, ajustando-se ao contexto normativo de apreensão da realidade como expressão da autonomia privada.

PALAVRAS-CHAVE

consentimento informado; saúde; pesquisa clínica; ato humano; proteção de dados pessoais; bioética.

---

154 Nota dos autores: Este texto hoje reunido e adaptado, foi originalmente foi publicado em três partes separadas, em datas diferentes entre setembro de 2021 a fevereiro de 2022 no site https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados.

155 Doutora em Direito (UFRGS) e Pós-Doutora em Medicina (UFRGS). Advogada - Sócia no Escritório Santana Fernandes Advocacia e Consultoria. Professora e Coordenadora Adjunta do Mestrado Profissional em Pesquisa Clínica do Hospital de Clínicas de Porto Alegre (HCPA). Pesquisadora Associada do Laboratório de Pesquisa em Bioética e Ética na Ciência do Centro de Pesquisas (LAPEBEC) do HCPA. Professora Colaboradora do PPG/Dir-PUCRS. Membro do Conselho do Instituto de Estudos Culturalistas – IEC. Research Fellow no UZH Digital Society Initiative - Universidade de Zurique, Suíça. Diretora de Privacidade e Proteção de Dados da ÁXIOS - Educação e Consultoria em Ética Ltda. CV http://lattes.cnpq.br/2132565174726788 - Instagram = @marciasantanafernandes - Twitter = @msfernandes

156 Biólogo, Doutor em Medicina e Consultor em Bioética. Chefe do Serviço de Bioética do HCPA. Professor Titular da Escola de Medicina da PUCRS. Professor Colaborador da Faculdade de Medicina da UFRGS. Professor do Mestrado Profissional em Pesquisa Clínica do Hospital de Clínicas de Porto Alegre (HCPA). Pesquisador responsável do Laboratório de Pesquisa em Bioética e Ética na Ciência do Centro de Pesquisas (LAPEBEC) do HCPA. Research Fellow no UZH Digital Society Initiative - Universidade de Zurique, Suíça. Diretor Sócio da ÁXIOS - Educação e Consultoria em Ética Ltda.

CV: http://lattes.cnpq.br/0485816067416121 - Instagram = @jrgoldim

The different consent processes in human research and health care and the Brazilian Data Protection Act

Márcia Santana Fernandes
José Roberto Goldim

ABSRACT

The health area involves different consent processes, which have distinct nature and purposes, as well as different legal effects. In this text the distinctions and points of connection between the consent process in the health area, both in clinical research and health care, involved adults and children and adolescents and the Brazilian General Data Protection Act - LGPD; Law 13.709/2018 are analyzed. This study is organized in three Parts: Part I deals with the consent process in clinical research (the one involving human beings); in Part II it deals with the consent process in health care, in particular considering the possibility of processing personal data in art. 7 and art. 11 of the LGPD, highlighting in particular the similarities and differences between the legal bases for the processing of personal data and the consent expressed in the context of health care and finally, in Part III, the consent process involving children and adolescents in situations of clinical research and in health care, as well as its relationship with the provisions of the LGPD is faced. The method used was a narrative literature review, based on texts published in Portuguese, English and Spanish. As a general conclusion, it should be noted that the human act of consent is directly connected to the exercise of freedom. The consent may represent different forms and meanings of will manifestation, having this act legal effects or not, adjusting itself to the normative context of apprehension of reality as an expression of private autonomy.

KEYWORDS

informed consent; health; clinical research; human act; personal data protection; bioethics.

Introdução

Consentir, verbo que contempla múltiplos sentidos e regências - dar consentimento, permitir, tolerar, condescender; demonstrar concordância; aquiescer; aprovar; concordar, etc.[157], está na essência e no sentido do tema que vamos tratar: o processo de consentimento. As palavras e os sentidos que nelas gravitam são os pontos de contato na rede do "universo normativo" e que também é o "universo narrativo" de conceitos, princípios, modelos normativos e hermenêuticos. Como diz Judith Martins-Costa em texto lapidar - *A concha do marisco abandonada e o nomos*:

> "(...) normatizar e inseparável do narrar". (...) Daí a importância de ter presente as narrações apreendidas nos diferentes códigos sociais, a inteligibilidade da conduta normativa repousando no "caráter comunitário *(comunal)* das narrações que fornecem o contexto desta conduta".[158]

O verbo consentir é o ponto de contato dos quatro pontos cardeais da Filosofia de Kant, incorporados pelas mãos de Savigny à Escola Histórica, e elevados por Augusto Teixeira de Freitas à trajetória do Direito Privado brasileiro[159]. São eles: 1) a ideia de liberdade, como um direito inato a todos os seres humanos, garantidora do pleno desenvolvimento de sua personalidade; 2) o entendimento da convivência social, como uma limitação reciproca de liberdades; 3) o respeito à pessoa humana, como base da justiça e fim da ordem social; e 4) a garantia do Direito, como condicionalidade dos arbítrios, para legitimar o emprego da coação material[160].

Consentir é ato humano diretamente conectado à liberdade, podendo representar diferentes sentidos e formas de manifestação de vontade, tenha este ato efeitos jurídicos ou não. No campo jurídico, a natureza do ato de consentir pode ser ato jurídico *stricto sensu* ou negócio jurídico, ajustando-se ao contexto normativo de apreensão da realidade como expressão da autonomia privada[161,162].

Ao longo dos tempos e da tradição social e jurídica, em particular na área da saúde, foram incorporados a este verbo múltiplos sentidos ou dele excluídos características e/ou efeitos sociais e jurídicos. A Bioética, a partir da década de 1970, concentra

---

[157] HOUAISS, Antônio; VILLAR, Mauro de Salles; MELLO FRANCO, Francisco Manoel de Mello. Dicionário Houaiss da língua portuguesa. Rio de Janeiro: Editora Objetiva, 1ª Edição, 2001, p. 807.

[158] MARTINS-COSTA, Judith. A concha do marisco abandonado e o *nomos; in* Narração e Normatividade – Ensaios de Direito e Literatura, MARTINS-COSTA, Judith (Cood.); São Paulo: Editora GZ, 2013, pgs. 8-11.

[159] TEIXEIRA DE FREITAS, Augusto. Consolidação das Leis Civis, 3ª Edição; p. XXXII, Rio de Janeiro, 1876.

[160] REALE, Miguel. A doutrina de Kant no Brasil (Notas à margem de um estudo de Clovis Bevilaqua). V. 42, p. 58-59. Revista da Faculdade de Direito, Universidade de São Paulo, 1947.

[161] CEZAR, Denise Oliveira. Pesquisa com medicamentos – aspectos bioéticos. São Paulo: Editora Saraiva, 2012, p. 178 e seguintes.

[162] HAICAL, Gustavo. A autorização no Direito Privado. Rio de Janeiro: Revista dos Tribunais, 2020. Recomendo esta obra a todos que desejem aprofundar a figura jurídica da autorização.

muitos estudos voltados ao consentimento na área da saúde, em particular na pesquisa envolvendo seres humanos.

Consentir é a "concha" receptora de sentidos; usando a delicada metáfora da "concha do marisco abandonado" empregada por Martins-Costa[163]:

> "(...) em uma concha jogada na areia da praia, o primitivo habitante que lhe recheava o conteúdo de há muito pode ter desaparecido e gerações de outros habitantes podem ali ter encontrado a sua morada".[164]

Ainda, destaco o sentido da utilização da palavra "processo" associada ao verbo "consentir"; aqui compreendido como uma cadeia de atos e/ou procedimentos, não necessariamente consecutivos ou postos de forma sequencial, que agregados ao ato de consentir lhe dão sentido e determinam os efeitos jurídicos.

O processo de consentir envolve elementos intrínsecos e elementos extrínsecos na perspectiva da pessoa natural que consente. Os elementos intrínsecos relacionados à condição ou a situação do consentidor, como a capacidade psicológico-moral e jurídica; as motivações subjetivas e/ou objetivas; e a forma, escrita ou verbal. Os elementos extrínsecos, aqueles postos pela situação concreta e jurídica, essenciais ao conhecimento do consentidor para respeitar os seus direitos informativos, de personalidade e de autodeterminação. O ato de consentir deve ser realizado sem inadequações éticas[165] e/ou vícios de consentimento (erro ou ignorância, dolo, coação e estado de perigo)[166].

O processo de consentimento é "o ritual clínico moderno da confiança"[167], seja na perspectiva bioética[168], moral e jurídica.[169,170].

Assim, considerando a mobilidade narrativa, de sentido e de interpretação jurídica do ato de consentir, se objetiva tratar, neste conjunto de textos, dos diferentes processos de consentimento na área da saúde. Este texto está organizado, em três partes: Parte I,

---

[163] MARTINS-COSTA, Judith. A concha do marisco abandonado e o nomos; in Narração e Normatividade – Ensaios de Direito e Literatura, MARTINS-COSTA, Judith (Cood.); São Paulo: Editora GZ, 2013, pgs. 8-11.

[164] MARTINS-COSTA, Judith. A concha do marisco abandonado e o nomos; in Narração e Normatividade – Ensaios de Direito e Literatura, MARTINS-COSTA, Judith (Cood.); São Paulo: Editora GZ, 2013, pgs. 8-11.

[165] GOLDIM, José Roberto Goldim. O consentimento informado numa perspectiva além da autonomia. Revista AMRIGS, Porto Alegre, 46(3,4): 109-116, jul.-dez. 2002. Também acessível na página https://studylibpt.com/doc/5084574/o-consentimento-informado-numa-perspectiva-al%C3%A9m-da

[166] Código Civil Brasileiro, Lei 10.406/2002; Capítulo IV – Dos Defeitos do Negócio Jurídico; artigos 138 ao 156 e Capitulo V – Da invalidade do Negócio Jurídico.

[167] WOLPE, Paul Root.The triumph of autonomy in American Bioethics: a sociological view. In: Raymond De Vires, Janardan Subedi. Bioethics and Society: constructing the ethical enterprise. Englewood Cliffs: Prentice-Hall, 1998, p. 49.

[168] GOLDIM, José Roberto Goldim. Consentimento, capacidade e alteridade. In: Giovana Benetti; André Rodrigues Corrêa; Márcia Santana Fernandes; Guilherme Monteiro Nitschke; Mariana Pargendler; Laura Beck Varela. (Org.). Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa. 1ed.Rio de Janeiro: GZ Editora, 2019, v. 1, p. 169-181.

[169] CEZAR, Denise Oliveira. Pesquisa com medicamentos – aspectos bioéticos. São Paulo: Editora Saraiva, 2012, p. 178 e seguintes.

[170] MARTINS-COSTA, Judith. A Boa-fé no Direito Privado – critérios para sua aplicação. São Paulo: Editora Marciel Pons, 2015, §21, p. 228-237.

trata do processo de consentimento na pesquisa[171] envolvendo seres humanos e os relativos à Lei Geral de Proteção de Dados – LGPD; Lei 13.709/2018; a Parte II trata das características do processo de consentimento na assistência à saúde e suas relações com o estabelecido na LGPD e por fim, na Parte III analisa, especificamente, o processo de consentimento envolvendo crianças e adolescentes em situações de pesquisa e em assistência na área da saúde, assim como a sua relação com o previsto na LGPD.

PARTE I – O PROCESSO DE CONSENTIMENTO NA PESQUISA ENVOLVENDO SERES HUMANOS E OS RELATIVOS À LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

1- Processo de Consentimento nas pesquisas clínicas envolvendo seres humanos.
As pesquisas clinicas envolvendo seres humanos são quaisquer estudos científicos que incluem pessoas, ou grupos de pessoas, que recebem intervenções com a finalidade de avaliar os efeitos relacionados à saúde.[172]

A pesquisa clínica é um gênero que abarca uma diversidade de projetos e estudos envolvendo seres humanos, conforme OMS[173]. Estas pesquisas podem ser chamadas também por sua espécie - os ensaios clínicos - isso é, quando ocorrem testes com a utilização, entre outros, de fármacos, células e produtos biológicos, procedimentos cirúrgicos, procedimentos radiológicos, dispositivos, tratamentos comportamentais, mudanças no processo de prestação de cuidados, inclusive preventivos.[174]

Particularmente, os ensaios clínicos são organizados, normalmente em duas etapas: pré-clínica e clínica.

A etapa pré-clínica envolve a utilização de modelos celulares e animais[175] ou simulações envolvendo modelos matemáticos. Excepcionalmente, ainda na etapa pré-clínica, podem ser realizados estudos de Fase 0 em seres humanos. São estudos com doses muito pequenas de uma molécula, que ainda está sendo desenvolvida, com finalidade de verificar se tem atividade biológica.

A etapa clínica, por outro lado, envolve diretamente seres humanos e está organizada em quatro fases, denominadas de fases I,II,III e IV. Os estudos de fase I avaliam a segurança da nova intervenção. Na fase II, além da segurança, é avaliada a tolerabilidade associada ao seu uso. Na fase III se agrega a avaliação da eficácia da intervenção. Finalmente, na Fase IV, quando o produto já está liberado para uso assistencial, além da segurança, da tolerabilidade e da eficácia, se avaliam os eventos decorrentes do seu uso

---

171 O uso da palavra pesquisa, utilizada no presente texto, é apresentando no sentido utilizado no Brasil, que tem o mesmo sentido da palavra investigação utilizado em Portugal.

172 Organização Mundial da Saúde (OMS), 2016, Clinical trials. http://www.who.int/topics/clinical_trials/en/, acessado em 30 setembro de 2016.

173 Organização Mundial da Saúde (OMS), 2016, Clinical trials. http://www.who.int/topics/clinical_trials/en/, acessado em 30 setembro de 2016.

174 Organização Mundial da Saúde (OMS), 2016, Clinical trials. http://www.who.int/topics/clinical_trials/en/, acessado em 30 setembro de 2016.

175 Regulada pela Lei 11.794/2008.

em larga escala e em situações de vida real. Estas fases são sucessivas e escalonadas, com níveis crescentes de volume de participantes, de complexidade e de exposição à nova intervenção.[176]

Neste contexto, o processo de consentimento, e sua respectiva formalização, é requisito obrigatório nos ensaios clínicos.[177,178] O processo de consentimento deve ser a expressão de uma conduta eticamente adequada, em respeito aos Direitos Humanos, Direitos Fundamentais e Direitos de Personalidade, em especial, em respeito aos princípios da confiança, da autonomia, autodeterminação e alteridade.[179,180].

Portanto, o processo de consentimento deve ser integrado em todas as fases 0, I, II, III e IV, da etapa clínica do projeto e protocolos de pesquisa clínica. O participante de pesquisa de cada fase tem que ser informado das finalidades, riscos, benefícios e direitos associados, para que possa participar do processo de tomada de decisão, com a compreensão devida, para exercer o poder (=potestativo) de aceitar, não aceitar ou desistir de sua participação.

O projeto de pesquisa clínica e os documentos que lhe acompanham, tais como protocolo de pesquisa, manual do pesquisador, termos de consentimento, termos de confidencialidade, termos específicos para regular o uso de dados de pesquisa e demais anexos necessários ao caso concreto, devem ser submetidos a avaliação de um ou mais Comitês de Ética em Pesquisa (CEPs).

Os CEPs devem ter composição multidisciplinar; ser credenciados às instancias governamentais e/ou institucionais que realizem pesquisa clínica e autorizados por regras de direito, autogestão e compliance. As atividades dos CEPs têm cunho avaliativo, consultivo e deliberativo, envolvendo a adequação ética, metodológica, de relevância e finalidade, de capacitação técnica e científica dos pesquisadores envolvidos e de compliance dos projetos realizados nas instituições de pesquisa. Os CEPs também podem estabelecer medidas concretas para evitar conflitos de interesse, em particular, os econômicos.

A necessidade da obtenção de consentimento dos participantes integra um conjunto de Boas Práticas Clínicas, mais conhecidas pela sigla em inglês GCP – Good Clinical

---

176 Goldim JR. A Avaliação Ética da Investigação Científica de Novas Drogas: A Importância da Caracterização Adequada das Fases da Pesquisa. Rev HCPA. 2007;27(1):66–73. Goldim, J. R. O consentimento informado e a adequação de seu uso na pesquisa em seres humanos. Tese (Doutorado em Medicina) - Faculdade de Medicina, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1999. p. 37.

177 Goldim, J. R. O consentimento informado e a adequação de seu uso na pesquisa em seres humanos. Tese (Doutorado em Medicina) - Faculdade de Medicina, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1999. p. 37.

178 Doyal, L.; Tobias, J. S. Informed consent in medical research. London: BMJ Books, 2001. p. 15-19.

179 Goldim, J. R. O consentimento informado e a adequação de seu uso na pesquisa em seres humanos. Tese (Doutorado em Medicina) - Faculdade de Medicina, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1999. p. 31. "Vale destacar que o Código de Nuremberg foi o primeiro documento com repercussão internacional que estabeleceu padrões éticos mínimos aceitáveis para a realização de projetos envolvendo seres humanos."

180 ESTADOS UNIDOS DA AMÉRICA. Trials of war criminal before the Nuremberg Military Tribunals (Nuremberg Code). Control Council Law, Washington, v. 10, p. 181-182, 1949.

Practice, que orientam um modelo normativo colgado em diferentes códigos sociais, de aceitação internacional, fruto da historicidade, em busca de limitar a *coisificação* dos seres humanos na realização de pesquisas em saúde e como forma de garantir a autonomia da vontade e privada dos participantes de pesquisa.

Inúmeros documentos relevantes regulam as atividades de pesquisa em seres humanos. A Declaração de Helsinki, originalmente de 1964[181] e hoje na sua 8ª Edição (2015), é uma referência fundamental. É um documento proposto pela Associação Mundial de Medicina (WMA), sem a força de ser um tratado ou legislação. Outras propostas de Boas Práticas Clínica envolvem as propostas pela European Medicines Agengy (EMA)[182]; pela Conferência Tripartite Internacional de Harmonização (ICH harmonised tripartite guidelines. Guideline for Good Clinical Practice E6 - R2)[183]; o Documento das Américas[184] e o Guia de Inspeção em Boas Práticas Clínicas (BPC) referente a ensaios clínicos com medicamentos e produtos biológicos – Guia n. 36/2020 proposto pela Agencia Nacional de Vigilância Sanitária (ANVISA).

No cenário nacional, no que concerne normatização de pesquisas envolvendo seres humanos, não há lei específica[185], mas a realização de pesquisas envolvendo os seres humanos deve respeitar os preceitos constitucionais, destacando-se o princípio norteador de todo o ordenamento, o princípio da dignidade da pessoa humana, os direitos fundamentais e sociais à saúde e a vedação de comercialização de partes do corpo, art. 199 §4ª. Também é regrado indiretamente por leis infraconstitucionais, entre elas o Código Civil Brasileiro, a Lei 10.406/2002 e a Lei 13.123/2015, que regula o acesso ao Patrimônio Genético.

O ano de 1988, marcado pela promulgação da Constituição Federal, também marca o início da regulamentação envolvendo pesquisa com seres humanos no país - a Resolução 01/1988 (revogada), publicada pelo Conselho Nacional de Saúde (CNS). Posteriormente, o marco regulatório brasileiro foi sendo alterado por duas diferentes vertentes:

1) No âmbito infralegal, as resoluções sobre pesquisa editadas Conselho Nacional de Ética em Pesquisa, via o Sistema CEP/CONEP, responsável pelo credenciamento dos CEPs no país e pela orientação de atividades em pesquisa clínica, destacamos: a Resolução 466/2012, que regula em geral a pesquisa envolvendo seres humanos na área da saúde; a Resolução 251/1997, que caracteriza as fases de pesquisa clínica e as Resoluções 441/2011 e 446/2012, relacionadas aos Biobancos.

---

[181] GOLDIM, José R.. Declaração de Helsinki I. Bioética. Acessível em https://www.ufrgs.br/bioetica/helsin1.htm

[182] Good Clinical Practice (GCP) - ICH guideline E6 (R2). Draft ICH principle https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice#current-version---revision-2-section

[183] Guideline for good clinical practice E6(R2) Current Step 4 version, 09 Nov 2016. https://www.ema.europa.eu/en/documents/scientific-guideline/ich-e-6-r2-guideline-good-clinical-practice-step-5_en.pdf

[184] BOAS PRÁTICAS CLÍNICAS: DOCUMENTOS DAS AMÉRICAS. IV Conferência pan-americana para harmonização da regulamentação farmacêutica. 2-4 de Março de 2005. https://bvsms.saude.gov.br/bvs/publicacoes/boas_praticas_clinicas_opas.pdf

[185] CRONGRESSO NACIONAL, Câmara de Deputados do Projeto de Lei 7082/2017 para regular a pesquisa com seres humanos.

2) As determinações da Agência Nacional de Vigilância Sanitário - ANVISA, por meio de Resoluções de Diretoria Colegiada (RDC), em particular destacamos a RDC 9/2011, RDC 10/2010 e RDC 38/2013. Estas resoluções são obrigatórias e o seu cumprimento deve ser observado por todos que realizem pesquisas clinicas no país.

Neste cenário, o processo de consentimento é exigido pelo sistema CEP/CONEP e também pela ANVISA nas situações de pesquisa clínica. Entendemos que este processo tem momentos essenciais: o primeiro concerne ao dever de informar à pessoa convidada para ser um participante de pesquisa, que deverá receber todas as informações para compreender as finalidades, os propósitos, os riscos, os benefícios, as condições e as salvaguardas à sua integridade física, moral e psicológica projetadas na pesquisa. A segunda é diretamente conectada ao acompanhamento do participante, durante e após a realização da pesquisa, para suporte e esclarecimento de quaisquer situações ou aspectos decorrentes da pesquisa. O terceiro relaciona-se ao estabelecimento de canais de comunicação adequados e seguros para fortalecer e ampliar os graus de entendimento do participante durante todo tempo em que este estiver envolvido com a pesquisa, e até mesmo após o seu término formal.

A capacidade de compreensão do participante deve ser ampla para que haja a validade do processo de consentimento. Ou seja, deve ser considerada a capacidade relacionada ao grau de desenvolvimento psicológico-moral e a capacidade jurídica[186].Portanto, a capacidade do participante deve ser avaliada e integrada durante todo assim como durante a realização da pesquisa, com a finalidade de avaliar as vulnerabilidades associadas. Para garantir a validade do processo, também deve ser considerada a forma utilizada para registrar o consentimento do participante, seja por meio de termo escrito e/ou de gravação de imagem e/ou voz.[187]

No que concerne a categoria jurídica do ato de consentimento, no contexto de pesquisa clínica, como diz Denise Oliveira Cezar, não tem natureza obrigacional ou contratual, mas sim pode ser para alguns um ato jurídico stricto sensu e para outros um negócio jurídico relacional, de natureza existencial, que nascerá com limites ao exercício da autonomia do participante às normas proibitivas, aos princípios de ordem pública e de bons costumes. Nas palavras da autora:

> "(...)é possível, que por meio de declarações, os titulares exerçam os seus direitos de personalidade, os quais poderão tomar a forma de atos jurídicos em sentido estrito ou negócios jurídicos, contanto não afetem o que têm de essencial."[188]

Denise Oliveira Cezar ressalta que a categoria dos negócios jurídicos relacionais, de natureza existencial, em um ambiente de ensaios clínicos, melhor caracteriza o con-

---

[186] GOLDIM, J. R. O consentimento informado numa perspectiva além da autonomia. Revista da Amrigs, Porto Alegre, v. 46, n. 3-4, p.109-116, jul./dez. 2002. p. 110.

[187] ALVES, Rainer G. de Oliveira.; FERNANDES, Márcia S.; GOLDIM, José Roberto. Autonomia, autoderterminação e incapacidade civil: uma análise sob perspectiva da Bioética e dos Direitos Humanos. R. Dir. Gar. Fund., Vitória, v. 18, n. 3, p. 239-266, set./dez. 2017. https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1128

[188] CEZAR, Denise Oliveira. Pesquisa com medicamentos – aspectos bioéticos. São Paulo: Editora Saraiva, 2012, p. 205.

sentimento do participante, pois estão presentes a liberdade de celebração e configuração; as declarações de vontade e os preceitos de autonomia privada; observa-se a função econômico-social das declarações e a integração a relações jurídicas de natureza relacional.

> "A qualificação do consentimento informado na pesquisa patrocinada de medicamentos como um negócio jurídico relacional, desta forma, apreende as características que revelam as semelhanças de família com o negócio jurídico, e também as suas peculiaridades jurídicas, com o que a interpretação do TCI, conquanto esteja sujeita às regras dos demais negócios, exige a prevalência de princípios adequados à natureza da relação jurídica."[189]

A irrenunciabilidade e indisponibilidade dos direitos de personalidade são elementos limitadores da liberdade e da autodeterminação do participante de pesquisa. Igualmente, os responsáveis pela pesquisa devem observar os direitos de personalidade do participante, sem submeter a qualquer influência de ordem hierárquica, ou a qualquer espécie de coerção, mesmo as de ordem econômica relacionadas a recebimentos de valores monetários elevados pela participação na pesquisa, ou recebimento de medicamentos ou tratamentos terapêuticos em ofensa a sua dignidade. [190]

A relação contratual - negócio jurídico de natureza patrimonial - é estabelecida entre os promotores e responsáveis pela pesquisa clínica, sejam patrocinadores e seus representantes, como as Organizações Representativas de Pesquisa Clínica (ORPC), ou, em inglês, *Contract Reserch Organization* (CRO), instituições que albergam a pesquisa, fundações de apoio e pesquisadores e suas equipes. O participante não é figurante no contrato, mas sim é pessoa diretamente interessada e afetada por esta relação contratual complexa, de natureza relacional.[191]

Assim, o consentimento do participante, registrado no Termo de Consentimento Livre e Esclarecido (TCLE) ou por outra forma de documentação, é elemento objetivo de formalização do processo do consentimento, que deve integrar o projeto de pesquisa, diretamente ligado ao contrato de pesquisa. O registro do consentimento deverá conter de forma clara, inteligível todos os aspectos necessários para informar o participante da finalidade, riscos, benefícios, direitos, titularidade dos responsáveis, contatos necessários para fluência da comunicação com o pesquisador responsável ou seu representante e as instituições.

Em algumas situações, poderá conter também explanação de como os dados de pesquisa serão tratados, se anonimizados, pseudonimizados ou indentificados e se serão

---

[189] CEZAR, Denise Oliveira. Pesquisa com medicamentos – aspectos bioéticos. São Paulo: Editora Saraiva, 2012, p. 199-231.

[190] GOLDIM, J. R. O consentimento informado e a adequação de seu uso na pesquisa em seres humanos. Tese (Doutorado em Medicina) - Faculdade de Medicina, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1999. p. 62. "A autonomia ocorre quando o indivíduo reconhece que as regras são mutuamente consentidas, as respeita e tem a noção de que podem ser alteradas."

[191] CEZAR, Denise Oliveira. Pesquisa com medicamentos – aspectos bioéticos. São Paulo: Editora Saraiva, 2012, p. 178 e seguintes.

compartilhados com outros grupos de pesquisa e/ou com patrocinadores ou financiadores da pesquisa. Nestas situações, a declaração do participante será específica para autorizar o uso de dados de pesquisa, quando originados de dados pessoais, atendendo aos requisitos da LGPD, artigo 8º. Este Termo deverá estabelecer a finalidade, a necessidade, o delineamento, os contornos, os limites e as medidas de segurança para o tratamento e divulgação dos dados de pesquisa. Ressalta-se que os responsáveis pela pesquisa serão controladores conjuntos, conforme os critérios da LGPD, artigo 5º, inciso VI. (ver item 2 deste texto).

Igualmente, é importante frisar que há situações de pesquisa clínica, excepcionais, que poderá haver a liberação da obtenção do consentimento. Por exemplo, quando houver a impossibilidade de estabelecer o contato com o participante, ou seu representante. Nesta situação, o projeto de pesquisa não poderá gerar danos ao participante, deverá ser garantido o tratamento de dados e informações de forma segura, e deverá ser comprovado, a priori, os impactos sociais positivos e benefícios decorrentes da pesquisa para a sociedade. Isto também pode ocorrer em situações nas quais os dados de pesquisa estejam anonimizados desde a sua origem. Nestas, ou em outras situações excepcionais, os pesquisadores devem solicitar e justificar, no projeto de pesquisa, encaminhado ao CEP para avaliação, esta dispensa de obtenção do consentimento. A avaliação do CEP deverá analisar as circunstâncias e as justificativas na perspectiva metodológica e de adequação ética, de boas práticas clinicas, legais e regulatórias.

A ética da responsabilidade social, expressa que a garantia do progresso da ciência e da tecnologia, em um espírito de cooperação, de difusão das informações científicas e de estímulo à livre circulação e utilização do conhecimento, somente se justifica se houver a proteção do participante como interesse primário. Esta proteção não pode ser um elemento secundário a outros interesses, sejam eles científicos, políticos ou econômicos[192].

Contudo, para que isso seja possível, é fundamental a transmissão adequada das informações e conhecimentos ao participante sobre a natureza, a finalidade, as etapas de desenvolvimento do projeto e sua prospectiva; assim como, as expectativas derivadas da pesquisa. O dever de informar do pesquisador e o direito de ser informado do participante da pesquisa, sob o fundamento no princípio da confiança, são elementos essencialmente relevantes ao processo de consentimento.[193,194]

---

[192] Jonas, H. Ética, medicina e ética. Lisboa: Vega-Passagens, 1994. p. 135.

[193] O´Neill, O. Autonomy and trust in bioethics. Cambridge: Cambridge University, 2002.

[194] FERNANDES, Márcia Santana. Bioética, Medicina e Direito de Propriedade Intelectual – relação entre patentes e células-tronco humanas. São Paulo: Editora Forense, 2012.

2- Processo de consentimento na LGPD

O consentimento da LGPD é uma de suas bases legal de tratamento, devendo ser considerado em políticas de proteção de dados e privacidade, mas não apenas como um processo de "faz de conta".[195] Neste sentido, será fundamental elencar três premissas postas na Lei Geral de Proteção de Dados, Lei 13.709/2018, diretamente relacionados às pesquisas envolvendo seres humanos na área da saúde:

2.1. O tratamento de dados pessoais (artigo 5º, inciso X) poderá ser realizado em situações de pesquisas, desde realizadas por órgão de pesquisa, artigo 5º, inciso XVIII (órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico);

2.2. A LGPD dispensa o consentimento, art. 8º, quando outras bases legais legitimarem o tratamento de dados, previstos no artigo 7º e 11. Dentre as situações de dispensa do consentimento, em situação envolvendo a área da saúde, destacamos do artigo 7º, os incisos IV (para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais) e VII (para a proteção da vida ou da incolumidade física do titular ou de terceiro) e do artigo 11, o inciso II, letra "a" (realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis) e a letra "e" (proteção da vida ou da incolumidade física do titular ou de terceiro).[196]

2.3. A LGPD autoriza no seu artigo 13 e parágrafos, o tratamento de dados pessoais para a realização de "estudos em saúde pública", diz o artigo que os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro. Este ambiente seguro deve ser de responsabilidade do controlador ou controladores (artigo 5º, inciso VI), que no caso das pesquisas clinicas são os pesquisadores e demais responsáveis pela pesquisa. As práticas de segurança devem estar previstas em regulamento específico e devem incluir, sempre que possível, a anonimização ou pseudonimização dos dados.

---

[195] LIMA, Cintia R. P. de. Políticas de proteção de dados e privacidade e o mito do consentimento. Migalhas, 15 de janeiro de 2021. https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/338947/politicas-de-protecao-de-dados-e-privacidade-e-o-mito-do-consentimento

[196] SARLET, Gabrielle B. S.; FERNANDES, Márcia S.; RUARO, Regina L.. A proteção de dados no setor da saúde em face do sistema normativo brasileiro atual in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

Partindo destas premissas legais, gostaríamos de focar em dois aspectos: i) a finalidade e a forma do processo de consentimento exigido pela LGPD são distintas dos necessários para a realização de pesquisas envolvendo seres humanos e ii) estes processos de consentimento não têm os mesmos efeitos jurídicos, nem são excludentes. Ambos podem ser necessários, conjuntamente ou não, de acordo com o caso concreto.

A finalidade e a forma do processo de consentimento informado exigido pela LGPD, no seu artigo 8º, são distintos do processo de consentimento necessário para a realização de pesquisas com seres humanos. O consentimento na LGPD é uma das bases legitimas de tratamento de dados pessoais e dados pessoais sensíveis, portanto os seus efeitos estão circunscritos a autorização do titular para o tratamento de dados e informações pessoais, em respeito aos seus direitos de personalidade e ao princípio da autodeterminação informativa. Portanto, entendemos que o consentimento na LGPD é um ato jurídico stricto sensu, pois sua forma, finalidade e efeitos estão previamente previstos em lei.

Para tratar dados de saúde, o consentimento da LGPD poderá ser dispensado para realização de assistência, proteger a integridade física e/ou de saúde do titular ou mesmo tratar o dado do titular em situações de pesquisa.[197] Entretanto, é importante que se diga, que dispensar o consentimento para tratamento de dados pessoais, nas situações previstas pela LGPD, não implica em ignorar os seus princípios e regras de direitos, em particular os princípios (artigo 6º) e os direitos dos titulares (dos artigos 17 ao 22).[198]

A dispensa do consentimento no caso de pesquisas pela LGPD, não altera as responsabilidades inerentes aos promotores e responsáveis pela pesquisa clínica (sejam patrocinadores, instituições envolvidas e pesquisadores responsáveis) em promover ambiente seguro para o tratamento de dados pessoais e dados pessoais sensíveis relacionados aos participantes no desenvolvimento da pesquisa. Aliás, os responsáveis da pesquisa, como controladores e/ou controladores conjuntos, devem elaborar e desenhar o projeto de pesquisa clinica contendo formas de tratamento e governança dos dados pessoais dos participantes para garantir a sua autodeterminação, inclusive para garantir a retirada do consentimento do participante ou o adequado compartilhamento ou mesmo o descarte dos dados.

Assim, devem ser previstas e organizadas no projeto e no contrato de pesquisa, por meio de cláusulas especificas, a definição dos obrigados e de medidas de segurança concretas, conforme exigidas pela LGPD para o tratamento dos dados pessoais dos participantes de pesquisa. Também devem ser estabelecidos controles e mecanismos para auditar as bases de dados e, sempre que possível, utilizar a pseudonimização ou outras técnicas de proteção dos dados de pesquisa que oriundos de dados e informações pessoais dos participantes.

---

[197] BARRETO, Mauricio L.; ALMEIDA, Bethânia; DONEDA, Danilo. Uso e proteção de dados pessoais na pesquisa científica, in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

[198] SARLET, Gabrielle B. S.; RUARO, Regina L.. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob enfoque da Lei Geral de Proteção de Dados(LGPD), Lei 13.709/2018. in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

Assim, os processos de consentimento não são excludentes, mas sim poderão ser necessários conjuntamente. Assim, a dispensa do consentimento pela LGPD, nas situações de pesquisa clinica, não elimina a exigência do processo de consentimento nos projetos de pesquisa clínica, visando a atender preceitos éticos, legais e regulatórios e às diretrizes de boas práticas clínicas, que devem ser avaliados pelo CEP.

Neste contexto, quando necessário também o consentimento da LGPD, este deve respeitar os requisitos do artigo 8º e poderá ser nominado como "termo de autorização para uso de dados de pesquisa" – inclusive constando em algumas situações como cláusulas contratuais "destacadas" (artigo 8º, § 1º). O termo poderá ser exigido quando houver situações em que os dados, identidade e informações dos participantes de pesquisa clínica tenham que ser divulgadas além dos limites previstos no projeto ou protocolos de pesquisa ou por situações particulares; como por exemplo, quando houver publicização das pesquisas em mídias sociais e jornalísticas; artigos científicos, congressos, ou para eventuais desenvolvedores de produtos e/ou tecnologias originadas das pesquisas, entre outras situações a serem analisadas em situações concretas.

3- Síntese conclusiva da Parte I

O consentimento do participante de pesquisa clínica deve atender a todos os requisitos formais e de conteúdo, como a clareza e legibilidade na linguagem, esclarecimento dos riscos e benefícios, possíveis eventos adversos, direitos, canais de contato, entre outros.

O consentimento previsto na LGPD, a princípio, não será exigido nos casos de pesquisas clínicas ou pesquisas em saúde pública, pois estas situações têm base legal própria, previstas na LGPD, para tratamento de dados pessoais. Da mesma forma, medidas de segurança devem ser tomadas pelos controladores dos dados de pesquisa, que são os responsáveis pela pesquisa, para garantir os níveis de proteção, prevenção, segurança, controle, gestão e verificação de dados e informações dos participantes, exigidas pela LGPD.

No entanto, poderão ocorrer situações, dependendo da finalidade e uso dos dados pessoais previstos no projeto de pesquisa, em que seja necessário que o participante de pesquisa também forneça o consentimento previsto na LGPD, registrado em "termo de autorização para uso de dados de pesquisa".

PARTE II – O PROCESSO DE CONSENTIMENTO NA ASSISTÊNCIA À SAÚDE E SUAS RELAÇÕES COM O ESTABELECIDO NA LGPD

A necessidade envolvida na assistência a saúde está relacionada a uma prestação de serviço que tem como objeto central os cuidados de saúde. Desta forma, o consentimento na assistência, por definição, envolve a relação profissional-paciente que é assimétrica, devido à vulnerabilidade associada ao assistido.[199] A obtenção do consentimento é um importante elemento de uma adequada relação profissional-paciente em ambientes assistenciais, sendo uma atividade intrínseca e fundamental, e não tangencial, à relação jurídica existente.

A assistência à saúde, aqui tratada, contempla o conceito de saúde proposto pela Organização Mundial da Saúde (OMS) - *estado de completo bem-estar físico, mental e social e não somente ausência de afecções e enfermidades* – e que hoje é central entre os Objetivos do Desenvolvimento Sustentável (ODS) e o Pacto Global da Organizações das Nações Unidas (ONU), portanto envolve todas as áreas da saúde e não somente a medicina. Também deve envolver necessariamente o tratamento de dados pessoais e dados pessoais sensíveis.

O processo de consentimento envolve diversas facetas do atual exercício dos cuidados em saúde. Este processo de consentimento não é apenas uma doutrina legal, é também um direito moral dos pacientes que gera obrigações legais e morais para os profissionais da área da saúde. O processo de consentimento pode assumir diferentes significados.

A relação jurídica estabelecida entre as partes tem como foco e objetivo central a assistência à saúde do assistido, pautada pela consideração que o direito à saúde é um direito fundamental e social, estabelecido nos artigos 5º e 6º da Constituição Federal e em demais regras de direito público e privado. A assistência à saúde pressupõe um negócio jurídico, que poderá conjugar deveres e obrigações contratuais ou existencial, entre o prestador dos serviços à saúde. O prestador poderá ser um ente público, com o por exemplo, a assistência efetivada pelo Sistema Único de Saúde (SUS); ou poderá ser uma pessoa jurídica de direito privado, como as clinicas e hospitais privados e filantrópicos, ou ainda, por uma pessoa natural, quando a assistência é realizada por um profissional liberal individualmente.

Neste contexto, e com o objetivo de integrar um conjunto de textos abarcando os diferentes processos de consentimento na área da saúde, passamos a tratar sobre aspectos característicos do processo de consentimento na assistência à saúde, em especial a sua natureza e efeitos jurídicos e, por fim, os pontos de contato com o estabelecido na à Lei Geral de Proteção de Dados – LGPD; Lei 13.709/2018.

[199] GENRO, B.; GOLDIM, J. R. Acreditação Hospitalar e o Processo de Consentimento Informado. Rev HCPA 2012;32(4).

1- Processo de Consentimento na assistência à saúde

1.1. A natureza jurídica do consentimento

A natureza jurídica do consentimento, em todos os seus sentidos, tem como fundamento e lastro o respeito ao princípio da dignidade da pessoa humana e da autodeterminação. Quanto a espécie caracteriza-se como um *ato jurídico lato sensu,* na sua variante de negócio jurídico. Pontes de Miranda ensina que *ato jurídico lato sensu* tem como seu suporte fático [=*o estudo das relações humanas e os fatos*] os seguintes elementos de composição: *exteriorização ou manifestação da vontade positiva (ação) ou negativa (omissão)* e um fim juridicamente pretendido e possível.[200] Esta espécie, pode assumir variantes, ou serão atos jurídicos em sentido stricto ou negócios jurídicos.

Os negócios jurídicos, espécie que interessa ao tema de estudo, tem como característica no núcleo de seu suporte fático a autonomia privada, quando a *vontade humana pode criar, modificar ou extinguir direitos, pretensões, ações ou exceções*.[201]

A categoria de negócio jurídico compreende apenas os tipos de atos humanos que, estruturados pelo ordenamento como suportes fáticos normativos, estão e são dirigidos finalisticamente para a constituição, modificação ou extinção de uma relação jurídica mediante o estabelecimento de uma norma jurídica que vincula as partes integrantes desta relação. *Portanto, o principal traço distintivo entre os atos não negociais e os negócios jurídicos está em que, nestes, há, conectada à ação humana, uma destinação voluntária polarizada pelo sentido de uma finalidade*. Em particular, na prestação de serviços de assistência o caráter finalista da ação subjacente ao negócio jurídico deve, pois, ser devidamente sublinhado. [202]

A prestação de assistência à saúde, o exercício dos deveres pelos prestadores, independentemente de sua natureza jurídica pública ou privada, deve ser pautado pela proteção da confiança e pressupõe que o bem jurídico ou a finalidade do negócio jurídico deve oferecer ao assistido o melhor tratamento ou acesso as tecnologias de saúde e também deve proteger a integridade envolvida nesta relação jurídica.

O princípio da confiança está na base das relações jurídicas, sejam de direito público ou privado, afirma Judith Martins-Costa.[203] Por sua vez, o princípio da proteção da

---

[200] PONTES DE MIRANDA, F. C. Tratado de Direito Privado, Parte Geral, Tomo I, p. 84. Rio de Janeiro: Editor Borsoi, 1954.

[201] PONTES DE MIRANDA, F. C. Tratado de Direito Privado, Parte Geral, Tomo III, p. 3. Rio de Janeiro: Editor Borsoi, 1954.

[202] MARTINS-COSTA, J.; FERNANDES, M. S.. Os biobancos e a doação do material biológico humano: um ensaio de qualificação jurídica. In: Bioética e Direitos Fundamentais, Org. Gozzo, D. e Ligieira, W. R.; São Paulo: Editora Saraiva, 2012.

[203] MARTINS-COSTA. Judith. A proteção da legítima Confiança nas Relações Obrigacionais entre a Administração e os Particulares. Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, UFRGS, Porto Alegre, n.22, pp.228-255, 2002.

confiança apresenta-se na dimensão individual, ou na vertente *subjetivada* da segurança jurídica.[204] Esse princípio, como indica Humberto Ávila, *depende do exercício da confiança*, com indicação concreta da quebra das expectativas de direito ou com a demonstração clara dos requisitos necessários à sua demonstração – *base da confiança, exercício da confiança e frustação da confiança.*[205]

O princípio da confiança, *tem o escopo imediato de assegurar expectativas*. Essas expectativas legitimadas *são como uma confiança objetivada* por uma situação de confiança, exigem como bem posiciona Denise Oliveira Cezar, os seguintes deveres por parte do prestador: dever de informar sobre os aspectos científicos, de procedimento, benefícios e riscos; definir a forma de cumprir com o dever; agir com prudência, perícia e diligência; agir em respeito as exigências éticas; respeito às Boas Práticas Clínicas; atenção aos usos e costumes da prática assistencial e ter constante atenção ao desenvolvimento do estado da arte, entendido como conhecimento científico atual. Por sua vez, estes deveres devem garantir ao assistido no mínimo os seguintes direitos, não limitados a estes: ser informado; manifestar suas escolhas de tratamento, inclusive assumindo os riscos, exceto em situações emergenciais; atender a interesse próprio; atender as orientações de tratamento.[206]

No contexto do SUS, a assistência a saúde representa um dever do Estado, além de ser um direito do cidadão, razão pela qual esta deve ser garantida por meio de *políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação* conforme a Constituição Federal, artigo 196, normatizada pela Lei 8080/1990, que estabelece o Sistema Único de Saúde (SUS), e permeada pelas ações e determinações da Agência de Vigilância Sanitária (ANVISA). Neste contexto, a relação não é propriamente balizada por uma relação contratual, mas sim como um dever do Estado em atender a preceito constitucional em respeito a sua missão e metas, gerando no assistido expectativas concretas em busca do melhor atendimento.

No âmbito do Direito Privado, as regras estão postas principalmente no Código Civil, Lei 10.406/2002; Código de Defesa do Consumidor, Lei 8078/1990, e regramentos da Agência Nacional de Saúde Suplementar (ANS), além das normas deontológicas que obrigam os profissionais nas suas respectivas áreas de atuação. Em todas elas, o processo de consentimento, balizado pelo princípio da confiança, é ancora. Na relação jurídica negocial, de natureza contratual, o prestador e o assistido são partes – figurantes na relação. O processo de consentimento integra a relação como um dever de prestação e como um direito do assistido. Igualmente, este processo deve ser dinâmico, contemplando mudanças no ato de consentir, correspondentemente no dever de informar, que possam ocorrer durante o vinculo, contemplando, inclusive, a necessidade de reconsentimento ou desistência de tratamento ou assistência.

---

[204] MARTINS-COSTA, J.. A Boa-Fé no Direito Privado – critérios para sua aplicação. Pag. 228-237. Paulo: Marcial Pons, 2015.

[205] ÁVILA, Humberto. Segurança Jurídica. Entre permanência, mudança e realização no Direito Tributário. Pag. 365; São Paulo: Editora Malheiros, 2011, p. 365.

[206] CEZAR, Denise Oliveira. Pesquisa com medicamentos - Aspectos Bioéticos. São Paulo: Editora Saraiva, 2012.

Cumpre alertar que a formalização do processo de consentimento em qualquer situação de assistência poderá ser realizada de várias formas, e não somente de forma escrita no termo de consentimento ou posta como cláusula aparte; poderá, por exemplo, ser feita verbalmente com anotações no prontuário do assistido; por meio de gravação de vídeo e voz quando da assistência por telemedicina, entre outras formas possíveis pelas tecnologias de informação e comunicação (TICs).

A validade do negócio jurídico, requer a capacidade civil e no caso do processo de consentimento também a validade ética, portanto é imprescindível avaliar se o indivíduo possui capacidade de tomar decisões no seu melhor interesse, considerando aspectos do seu desenvolvimento psicológico moral. Esta característica envolve, também, o entendimento das informações fornecidas para que possa escolher a melhor alternativa, desde o seu ponto de vista.[207]

O exercício dos direitos do assistido no processo de tomada de decisão perpassa necessariamente pela adequada comunicação e recebimento de informações acessíveis para o entendimento (considerando graus de instrução e competências intelectuais). As informações devem ser suficientes para que possa tomar decisões. Devem ser prestadas as informações consideradas essenciais para o adequado entendimento. O volume excessivo de informações pode prejudicar a própria compreensão do que de fato está sendo compartilhado. Da mesma forma, é dever dos profissionais envolvidos ter pleno domínio dos conteúdos de informação transmitidos, pois os pacientes/assistidos e familiares se baseiam muito mais nas informações verbais prestadas do que no conteúdo escrito em documentos. Portanto, coerência entre o que é dito e o que está, por ventura, escrito, é fundamental.[208]

O respeito à autonomia e à dignidade de cada um é um imperativo ético e não um favor que podemos ou não conceder uns aos outros, já ensinou Paulo Freire. Este ensinamento cabe para todos os indivíduos, especialmente para àqueles que atuam na área da saúde, pois fornecer informações e acompanhar o processo de tomada de decisão, suprindo com esclarecimentos necessários, é que dará sentido ao processo de consentimento e permitirá a autodeterminação do assistido, protegendo o exercício de sua autonomia e dignidade.[209] Portanto, o instituto da representação deve conformar as situações envolvendo incapacidade legal ou mesmo de falta de discernimento do assistido para tomar decisões sobre seu cuidado ou em seu melhor interesse. A validade jurídica e bioética do ato de consentir deve considerar, também, a cultura e costumes dos assistidos e as peculiaridades envolvidas na tomada de decisão. Em algumas situações específicas, o assistido também pode estar prejudicado em sua capacidade para decidir,

---

[207] GENRO, B.; GOLDIM, J. R.. Acreditação Hospitalar e o Processo de Consentimento Informado. Rev HCPA 2012;32(4).

[208] GENRO, B.; GOLDIM, J. R.. Acreditação Hospitalar e o Processo de Consentimento Informado. Rev HCPA 2012;32(4).

[209] Bittencourt, A. L. P.; Quintana, A. M.; Velho, M. T. A. de C. ; Goldim, J.R.; Wottrich, L. A. F.; Cherero, E. de Q. A voz do paciente: por que ele se sente coagido? Psicologia em Estudo, Maringá, v. 18, n. 1, p. 93-101, jan./mar. 2013.

como por exemplo, nas situações de emergência ou de restrição de autonomia devido a condições clínicas.[210]

Igualmente, deve ser atentado a distinção entre voluntariedade e autonomia na perspectiva da Bioética, pois estes são conceitos que se diferenciam por uma linha tênue, como explica Goldim e colaboradores em estudos sobre coerção na assistência a saúde[211]:

> O exercício da voluntariedade se dá ao longo da tomada de decisões, pela minimização de qualquer forma de constrangimento ou coerção. Uma decisão voluntária é aquela tomada livre de qualquer influência ou pressão; já a decisão autônoma é aquela tomada por um sujeito capaz de decidir sobre o que é melhor para si. Uma escolha só poderá ser considerada autônoma se for voluntária, ou seja, se a pessoa estiver livre de qualquer influência.

Ainda, pode-se demonstrar *a percepção de coerção,* como o oposto da percepção de autonomia do assistido, e um conceito diferente da *coerção propriamente dita* na área da saúde. A análise de coerção e de percepção de coerção não supera a necessária análise jurídica de invalidade do negócio jurídico quanto aos seus defeitos, conforme previstos no Código Civil, como os casos de erro ou ignorância (artigos 138 a 144), dolo (artigos 145 a 150)[212], coação (artigos 151 a 155), estado de perigo (artigo 156) e simulação (artigo 168) ou mesmo outros requisitos de validade, postos no artigo 104.

O princípio da boa-fé é transversal e vai atingir tanto o processo de consentimento na assistência pelo Estado, que deve observar este princípio basilar, como nas relações de Direito Privado, conforme previsão do Código Civil, artigo 113 e do Código de Defesa do Consumidores, artigo 4º, inciso III.

1.2. A assistência a saúde via Telemedicina e o processo de consentimento

A telemedicina é uma importante prática na dinamização e ampliação do acesso e atenção à saúde da população. Conforme definido na Resolução do CFM 1643/2002, artigo 1º, *a Telemedicina como o exercício da Medicina através da utilização de metodologias interativas de comunicação audiovisual e de dados,* possui *o objetivo de assistência, educação e pesquisa em Saúde*. [213]

Os benefícios potenciais da telemedicina, destacados pela Declaração de Tel Aviv, referem-se à possibilidade de os pacientes terem maior acesso a prestações de especialistas, ou mesmo da atenção básica, pois: *a telemedicina permite a transmissão de*

---

[210] GENRO, B.; GOLDIM, J. R.. Acreditação Hospitalar e o Processo de Consentimento Informado. Rev HCPA 2012;32(4).

[211] BITTENCOURT, A. L. P.; QUINTANA, A. M.; VELHO, M. T. A. DE C. ; GOLDIM, J.R.; WOTTRICH, L. A. F.; CHERERO, E. DE Q. A voz do paciente: por que ele se sente coagido? Psicologia em Estudo, Maringá, v. 18, n. 1, p. 93-101, jan./mar. 2013. Em outro estudo: WITTMANN-VIEIRA, R.; GOLDIM, J. R.. Percepção de coerção de pacientes submetidos a procedimento médico invasivo. Rev. Bioét. vol.27 no.4 Brasília Out./Dez. 2019. Doi: 10.1590/1983-80422019274351

[212] Para os estudos sobre dolo no Direito Civil, ver: BENETTI, Giovana. Dolo no Direito Civil – uma análise da omissão de informações. São Paulo: Quartier Latin, 2019.

[213] CONSELHO FEDERAL DE MEDICINA-CFM. Resolução do CFM 1643 de 26 de agosto de 2002. https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643

imagens médicas para realizar uma avaliação à distância em especialidades tais como radiologia, patologia, oftalmologia, cardiologia, dermatologia e ortopedia. Essas medidas podem facilitar os serviços do especialista, ao mesmo tempo em que diminuem os possíveis riscos e custos relativos ao transporte do paciente e/ou à imagem de diagnóstico.[214]

Os sistemas de comunicações, como a videoconferência e o correio eletrônico, conforme a Declaração de Tel Aviv, permitem aos médicos, de diversas especialidades, consultar colegas e interagir com pacientes com maior frequência e manter excelentes resultados dessas consultas (Art. 2). Os princípios ditados nessa declaração têm a função precípua de proporcionar um primeiro quadro de referência para uma utilização adequada da telemedicina. Por essa razão, a Associação Médica Mundial propõe revisar, de forma periódica, a adequação dos problemas que possam surgir nesse campo com o intuito de garantir a conformidade com os avanços tecnológicos e a ética médica, estabelecidos no *WMA Statement on ethics of telemedicine*, expresso na 58ª Assembleia Geral, em 2007, emendada na 69ª Assembleia, em 2018[215], em outras palavras, recomendou:

1. A telemedicina deve ser adequadamente adaptada às estruturas reguladoras locais, que podem incluir o licenciamento de plataformas de telemedicina no melhor interesse dos pacientes.
2. Quando apropriado, a WMA e as Associações Médicas Nacionais devem incentivar o desenvolvimento de normas éticas, diretrizes de prática, legislação nacional e acordos internacionais sobre assuntos relacionados à prática da telemedicina, enquanto protegem o relacionamento médico-paciente, a confidencialidade e a qualidade dos cuidados médicos.
3. A telemedicina não deve ser vista como igual à assistência médica presencial e não deve ser introduzida apenas para reduzir custos ou como um incentivo perverso à prestação excessiva de serviços e aumento de ganhos para os médicos.
4. O uso da telemedicina requer que a profissão identifique e gerencie explicitamente as consequências adversas nos relacionamentos colegiais e nos padrões de referência.
5. Novas tecnologias e estilos de integração de práticas podem exigir novas diretrizes e padrões.
6. Os médicos devem fazer *lobby* por práticas éticas de telemedicina que sejam do melhor interesse dos pacientes.

---

[214] BOTRUGNO; Carlo; GOLDIM, José Roberto; FERNANDES, Márcia Santana. The telehealth Brasil networks: A "socially engaged" technological system. ISSN: 2175_2990 | Latin Am J telehealth, Belo Horizonte; 6 (1): 044 – 058, 2019.

[215] WORLD MEDICAL ASSOCIATION -WMA. Statement on ethichs of telemedicine, expresso no 58ª Assembleia Geral em 2007, emendada na 69ª Assembleia, em 2018. Acessível em: https://www.wma.net/policies-post/wma-statement-on-the-ethics-of-telemedicine/

Assim, a telemedicina deve, em todos os tempos, de urgência ou não, buscar reduzir as distâncias, oferecendo apoio à assistência à saúde de qualidade e ampliando o acesso, os recursos e as informações científicas e deve refletir sobre a melhor forma de estabelecer o processo de consentimento informado.

É relevante destacar que os dados e informações utilizados são dados pessoais de pacientes, por isso, o seu uso deve ser autorizado, consentido e devem existir protocolos assistenciais específicos para essa espécie de atendimento, assim como o devido registro em prontuário eletrônico.[216]

2- Consentimento informado na LGPD e o tratamento de dados pessoais e sensíveis em saúde

O consentimento informado da LGPD é uma de suas bases legal de tratamento, devendo ser considerado em políticas de proteção de dados e privacidade de instituições de saúde; consultórios ou escritórios de profissionais liberais; e particularmente serem previstas pela Administração Pública que lida com dados de saúde.

Assim, partimos de duas premissas da Lei Geral de Proteção de Dados, Lei 13.709/2018, diretamente relacionados a assistência à saúde, quanto ao tratamento de dados pessoais e dados pessoais sensíveis: 1) por meio de consentimento informado específico, artigos 7º, inciso I (mediante o fornecimento de consentimento pelo titular); 8º e 11, inciso I (quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas) e 2) por meio de dispensa o consentimento, quando outras bases legais legitimarem e justificarem o tratamento de dados, também previstos nos artigos 7º e 11.

No que concerne, as situações de dispensa do consentimento em situação envolvendo a área da saúde, destacamos: o artigo 7º, incisos V (quando necessário para execução de contratos); VII (para a proteção da vida ou da incolumidade física do titular ou de terceiro) e VIII (para tutela da saúde, exclusivamente, em procedimentos realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária); e o artigo 11, o inciso II, letra "a" (cumprimento de obrigação legal ou regulatória pelo controlador); "b" (tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos) e a letra "e" (proteção da vida ou da incolumidade física do titular ou de terceiro).[217]

Partindo destas premissas legais, como fizemos na Parte I, gostaríamos de focar em dois aspectos: i) a finalidade e a forma do processo de consentimento exigido pela LGPD são distintas dos envolvidos no processo de consentimento na assistência e ii) estes processos de consentimento, a exemplo do que ocorre com a pesquisa envolvendo seres

---

[216] Para informações sobre a situação referente a telemedicina no Brasil, ver: TELESSAÚDERS-UFRGS é um núcleo de pesquisa vinculado ao Programa de Pós-Graduação em Epidemiologia da Faculdade de Medicina da Universidade Federal do Rio Grande do Sul (UFRGS). Acessível em: https://www.ufrgs.br/telessauders/; BOTRUGNO; Carlo; GOLDIM, José Roberto; FERNANDES, Márcia Santana. The telehealth Brasil networks: A "socially engaged" technological system. ISSN: 2175_2990 | Latin Am J telehealth, Belo Horizonte; 6 (1): 044 – 058, 2019; FERNANDES, Márcia Santana Fernandes. Slippery Slope: The Tracking of Personal Data and Covid-19. In Biothics & Neuroethics in Global Pandemic Times, org. Oliveira, Nythamar de; Castanheira, Nuno e Tauchen, Jair, 2020. Acessível m https://www.fundarfenix.com.br/64-bioethics-neuroethics

[217] SARLET, Gabrielle B. S.; FERNANDES, Márcia S.; RUARO, Regina L.. A proteção de dados no setor da saúde em face do sistema normativo brasileiro atual in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

humanos, não têm os mesmos efeitos jurídicos, nem são excludentes, dependendo do caso concreto.

Reforçando nosso entendimento, a finalidade e a forma do processo de consentimento informado exigido pela LGPD, no seu artigo 8º, são distintos do processo de consentimento necessário para a realização de assistência em saúde ou mesmo em pesquisas com seres humanos.

O consentimento na LGPD é uma das bases legitimas de tratamento de dados pessoais e dados pessoais sensíveis, portanto os seus efeitos estão circunscritos a autorização do titular para o tratamento de dados e informações pessoais, em respeito aos seus direitos de personalidade e ao princípio da autodeterminação informativa. Portanto, entendemos que o consentimento na LGPD é um ato jurídico stricto sensu, pois sua forma, finalidade e efeitos estão previamente previstos em lei e como vimos tem natureza jurídica distinta do processo de consentimento para finalidades de consentir na assistência a saúde – que tem a natureza de um negócio jurídico, conforme já tivemos a oportunidade de mencionar no item II.1 deste texto.

Para tratar dados de saúde, o consentimento da LGPD poderá ser dispensado para realização de assistência, proteger a integridade física e/ou de saúde do titular ou mesmo tratar o dado do titular em situações de pesquisa.[218] Entretanto, é importante que se diga, que dispensar o consentimento para tratamento de dados pessoais, nas situações previstas pela LGPD, não implica em ignorar os seus princípios e regras de direitos, em particular os princípios (artigo 6º) e os direitos dos titulares (dos artigos 17 ao 22).[219]

A dispensa do consentimento para tratamento de dados previsto na LGPD, não exclui o dever de prestadores de serviços e responsáveis pela assistência em saúde promover o devido processo de consentimento para realização da assistência. Da mesma forma, não altera as responsabilidades inerentes a estes prestadores em promover uma infosfera[220] segura para o tratamento de dados pessoais e dados pessoais sensíveis relacionados aos participantes no desenvolvimento da pesquisa. Aliás, os responsáveis pela assistência são controladores e/ou controladores conjuntos, devem elaborar e promover formas de tratamento e governança dos dados pessoais que garantam a sua autodeterminação. O princípio da boa-fé objetiva também aqui é transversal, com todas as consequências jurídicas, conforme previsão do artigo 6º da LGPD.

O princípio da autodeterminação será observado e respeitado com a promoção de acesso seguro ao prontuário eletrônico. A tecnologia de blockchain, por exemplo, vem sendo testada e na pesquisa na área da saúde para permitir a interoperabilidade dos sistemas de prontuários eletrônicos, com o objetivo de permitir, simultaneamente, o

---

218 BARRETO, Mauricio L.; ALMEIDA, Bethânia; DONEDA, Danilo. Uso e proteção de dados pessoais na pesquisa científica, in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

219 SARLET, Gabrielle B. S.; RUARO, Regina L.. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob enfoque da Lei Geral de Proteção de Dados(LGPD), Lei 13.709/2018. in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

220 FLORIDI, Luciano. The Ethics of Information. Oxford (UK): Oxford University Press, 2013.

estabelecimento de um registro com índice único e acesso distribuído, mas garantindo a segurança e a privacidade dos pacientes.[221] A tecnologia de blockchain, como já tivemos a oportunidade de mencionar, caracteriza-se por permitir que haja um registro distribuído, tendo como medida de segurança o acesso de forma descentralizada, não unificados, por meio de blocos, contendo dados e informações, que podem ser agregados de forma linear e cronológica, adicionando-se ao todo como um lego. Assim, vários novos nós vão sendo criados à medida que novos blocos vão sendo agregados.[222]

Assim, devem ser estabelecidos controles e mecanismos para auditar as bases de dados e, sempre que possível, utilizar a pseudonimização ou outras técnicas de proteção dos dados de pesquisa que oriundos de dados e informações pessoais dos participantes. As notícias recentes sobre o vazamento de dados do sistema ConenteSUS[223], é exemplo do importante papel que terá a Autoridade Nacional de Proteção de Dados (ANPD) e o Poder Judiciário, quando demandado, para regular esta questão e estabelecer uma relação de equilíbrio e segurança jurídica.

Os processos de consentimento não são excludentes, mas sim poderão ser necessários de forma conjunta. Assim, a dispensa do consentimento pela LGPD, nas situações de assistência, não elimina a exigência do processo de consentimento de assistência, dever que integra o negócio jurídico de prestação de serviços em saúde, seja pelo poder público ou pela iniciativa privada, visando a atender preceitos éticos, legais e regulatórios e às diretrizes de boas práticas, previstas em regras deontológicas, conforme dissemos.

Neste contexto, quando necessário também o consentimento da LGPD, este deve respeitar os requisitos do artigo 8º e poderá ser nominado como "termo de autorização para uso de dados de pessoais" – inclusive constando em algumas situações como cláusulas contratuais "destacadas" (artigo 8º, § 1º). O termo poderá ser exigido quando houver situações em que os dados, identidade e informações dos assistidos tenham que ser utilizados, divulgados e tratados para outros fins que ultrapasse a finalidade assistencial, como p. ex. quando houver publicização em mídias sociais e jornalísticas; artigos científicos, congressos, ou para eventuais desenvolvedores de produtos e/ou tecnologias em saúde, entre outras situações a serem analisadas em situações concretas.

O consentimento é essencial nos negócios jurídicos de prestação de serviços, que envolvam tratamento de dados pessoais para finalidades precisas, como de assistência à saúde ou previdência entre indivíduos, empresas privadas de telefonia ou de empresas como a Google; Facebook, Twitter, Youtube, Yahoo, entre outras, situação que necessariamente exige o consentimento informado, previsto no artigo 8º da LGPD.

---

[221] ROEHRS, A. ; DA COSTA, C. A.; DA ROSA RIGHIA, R., DA SILVA, V.F. , GOLDIM, J.R; SCHMIDT, D.C. Analyzing the performance of a blockchain-based personal health record implementation, J Biomed Inform. 2019 Apr;92:103140. doi: 10.1016/j.jbi.2019.103140. Epub 2019 Mar 4.(2019).

[222] FERNANDES, M. S.; GOLDIM, J.R. A sistematização de dados e informações em saúde em um contexto de big data e blockchain, in Lucca, N.; Pereira de Lima, C.R.; Simão, A.; Dezem, R.M.M.M (Org). Direito e Internet IV, no prelo, prevista publicação para 2019.

[223] A situação foi amplamente divulgada pela mídia, os vazamentos ocorreram em fevereiro de 2021 e em dezembro de 2021, por duas vezes consecutivas expondo os dados de saúde de mais de 190 milhões de pessoas. Inclusive a ANPD cobrou explicações do Ministério da Saúde, ver em: https://www.uol.com.br/tilt/noticias/redacao/2021/12/11/anpd-cobra-explicacoes-do-ministerio-da-saude-apos-ataque-cibernetico.htm

3- Síntese conclusiva Parte II

O ato de consentir deve ser reconhecido e examinado em cada uma das situações empregadas, atendendo ao sentido, finalidade e características jurídicas próprias, considerando a diversidade das situações para proteger e garantir o assistido o respeito aos seus direitos.

O consentimento informado da LGPD e o processo de consentimento inerente aos negócios jurídicos de prestação de serviços e assistência em saúde, observado as suas distinções de natureza jurídica e de finalidade, devem atender a todos os requisitos formais e de conteúdo, como a clareza e legibilidade na linguagem, esclarecimento dos riscos e benefícios, possíveis eventos adversos, direitos, canais de contato, entre outros,

Não será exigido nos casos assistência à saúde, a princípio, o consentimento informado previsto no artigo 8º da LGPD, pois as situações envolvidas na assistência têm base legal própria que autorizam o tratamento de dados pessoais e dados pessoais sensíveis.

Em todos os casos, seja o tratamento de dados de dados pessoais e sensíveis para situações ou correlacionadas à assistência em saúde baseado ou não no consentimento informado, previsto nos artigos 7º, inciso I; 8º e 11, inciso I, da LGPD, medidas de segurança devem ser tomadas pelos controladores, que são responsáveis pelo tratamento, para garantir os níveis de proteção, prevenção, segurança, controle, gestão e verificação de dados e informações dos participantes, exigidos pelo princípio da boa-fé objetiva.

Enfim, além de ter um Termo de Consentimento assinado, é fundamental documentar adequadamente o processo de consentimento nos prontuários dos pacientes. Sempre vale lembrar o que Pedro Abelardo propôs no século 12, que o valor moral de uma ação depende da intenção de quem a realiza e do consentimento de quem a sofre.

PARTE III - OS DIFERENTES PROCESSOS DE CONSENTIMENTO NA PESQUISA ENVOLVENDO CRIANÇAS E ADOLESCENTES E NA LGPD

O ato humano de consentir está diretamente conectado ao exercício da liberdade. O consentimento pode representar diferentes formas e sentidos de manifestação de vontade, tendo este ato efeitos jurídicos ou não, ajustando-se ao contexto normativo de apreensão da realidade como expressão da autonomia privada, conforme afirmamos na Parte I, deste texto.

Relembramos o leitor, para manter o fio condutor das Partes I, II e III deste texto, que partirmos do entendimento que o ato de consentir na área da saúde, seja na assistência ou na pesquisa clínica, está integrado a um processo, composto de elementos intrínsecos e extrínsecos na perspectiva da pessoa que consente. Dissemos na Parte I:

> Os elementos intrínsecos relacionados à condição ou a situação do consentidor, como a capacidade psicológico-moral e jurídica; as motivações subjetivas e/ou objetivas; e a forma, escrita ou verbal. Os elementos extrínsecos, aqueles postos pela situação concreta e jurídica, essenciais ao conhecimento do consentidor para respeitar os seus direitos informativos, de personalidade e de autodeterminação. O ato de consentir deve ser realizado sem inadequações éticas[224] e/ou vícios de consentimento (erro ou ignorância, dolo, coação e estado de perigo)[225].

1.Os elementos intrínsecos do Processo de Consentimento

Os elementos intrínsecos do processo de consentimento relacionam-se às características da pessoa do consentidor. Os três pilares que fundamentam o processo de consentimento são: o estágio de desenvolvimento psicológico-moral; o discernimento mental e a capacidade jurídica.

A pessoa, ao longo de sua vida, transita por diferentes estágios de desenvolvimento psicológico-moral. Estes são condicionados e também condicionantes da forma de como a decisão individual será baseada, considerando as diversas habilidades e percepções normativas de cada um. Entre as habilidades é possível destacar o envolvimento com o assunto, a identificação e a compreensão das alternativas e a comunicação de suas preferências. A percepção normativa se estende desde a perspectiva social até a jurídica. Portanto, a validade moral e legal do processo de consentimento deve atentar para as características da autonomia psicológica envolvida na ação, na racionalidade e na independência da pessoa do consentidor.

A participação de crianças e adolescentes no processo de consentimento na área da pesquisa e na assistência à saúde deve ser incentivada de acordo com o desenvolvimento psicológico-moral, isto é, da sua autonomia. Esta adequação do processo deve reconhecer os diferentes estágios biopsicossociais envolvidos e a sua justificativa de validade moral, ainda que pendente de uma validade jurídica[226].

---

[224] GOLDIM, José Roberto Goldim. O consentimento informado numa perspectiva além da autonomia. Revista AMRIGS, Porto Alegre, 46(3,4): 109-116, jul.-dez. 2002. Também acessível na página https://studylibpt.com/doc/5084574/o-consentimento-informado-numa-perspectiva-al%C3%A9m-da

[225] Código Civil Brasileiro, Lei 10.406/2002; Capítulo IV – Dos Defeitos do Negócio Jurídico; artigos 138 ao 156 e Capitulo V – Da invalidade do Negócio Jurídico.

[226] RAYMUNDO MM, GOLDIM JR. Moral-psychological development related to the capacity of adolescents and elderly patients to consent. J Med Ethics. 2008;34:602–5.

O processo de consentimento, no que concerne ao discernimento mental deve considerar a situação concreta e a sua relação o desenvolvimento psicológico-moral do individuo, assim como a sua eventual vulnerabilidade social. Estes quatro estágios de consciência sobre as normas sociais e jurídicas são: a anomia, a heteronomia, a autonomia e a socionomia. Cada um destes estágios indica a relevância e a compreensão da informação para as pessoas e a base na qual o consentimento será fornecido ou não.[227]

Para as pessoas no estágio de anomia, as informações disponíveis e fornecidas não são relevantes, na medida em que a capacidade de compreensão de normas é inexistente. Estas manifestações ocorrem por impulsos e reflexos; por exemplo, um bebê chora e se movimenta ao demonstrar contrariedade ou desconforto, quando é manipulado em um exame médico ou recebe uma injeção.

As pessoas no estágio de heteronomia não questionam as informações disponíveis, elas simplesmente as aceitam, por falta de possibilidade de exercerem a sua autodeterminação sejam elas de ordem emocional, psicológica ou física. A heteronomia ocorre em situações marcadas pelo constrangimento, coação ou submissão.

O estado de heteronomia também envolve, na área da saúde, as situações denominadas de "heterodeterteminação bioeticamente orientada". Expressão cunhada por Judith Martins-Costa para os casos de pessoas, que apesar de terem capacidade jurídica, são incapazes mentalmente, de tomar decisões em prol de seu melhor interesse.[228] Esta situação é associada a comportamentos caracterizados como sendo paternalistas.

Ao contrário do estado da heteronomia, as pessoas em estágio de autonomia, questionam as informações disponíveis e fornecidas. Neste estágio existe a possibilidade de haver autodeterminação, ou seja, as decisões apresentam-se de forma individual e consciente. Na área da saúde, existe a pressuposição de que as deliberações envolvem pessoas autônomas que têm condições de tomar decisões em prol de seu melhor interesse.

Por fim, para as pessoas no estágio de socionomia, as informações, além de serem compreendidas, são compartidas. Existe uma confiança recíproca entre os participantes. O emissor da informação, que compartilha orientações é responsável também por desencadear o processo de consentimento. Por outro lado, o consentidor é o receptor das informações, é quem toma as decisões baseando-se nas orientações recebidas e nas alternativas associadas. As deliberações em saúde, quando realizadas no estágio de Socionomia, decorrem da autonomia e da autodeterminação dos participantes, realizadas de forma dialogada e integrada. Na realidade, é uma decisão efetivamente compartilhada entre todos os envolvidos no processo.

---

[227] Goldim, J. R. Bioética: origens e complexidade. Revista HCPA, Porto Alegre, v. 26, n. 2, p. 86-92, 2006. Ver também GOLDIM, José Roberto. Autonomia e autodeterminação: confusões e ambiguidades.In: Judith Martins-Costa (coord). Conversa sobre autonomia privada.Canela: IEC, 2015.

[228] MARTINS-COSTA, Judith. Capacidade para consentir e esterilização de mulheres tornadas incapazes pelo uso de drogas: notas para uma aproximação entre a técnica jurídica e a reflexão bioética. In: Judith Martins-Costa; Letícia Ludwing Möller (Org.). Bioética e responsabilidade. Rio de Janeiro: Forense, 2009; p. 339.

Quadro sistematizado dos estágios de consciência da regra, Goldim (2006)

Estágio de consciência da regra	Informações disponíveis ao individuo	Autorização baseada na situação do indivíduo
Anomia	Não relevante	Impulso
Heteronomia	Não questionável	Constrangimento
Autonomia	Questionável	Decisão individual
Socionomia	Compreensíveis	Confiança recíproca

O terceiro pilar deste processo é a capacidade jurídica, pautada em uma determinação legal de critérios de idade ou de estado da pessoa, que condiciona a validade jurídica e o exercício da liberdade de escolha e autonomia. A Teoria das Incapacidades no Direito Civil Brasileiro considera crianças e adolescentes, menores de 18 anos, como sendo incapazes civilmente. Por isso necessitam representação legal - representação de genitores, tutores ou curadores - para que os atos jurídicos praticados sejam considerados válidos.

Os Direitos de Crianças e Adolescentes, apesar de tardios no mundo, assim como no Brasil, se estruturam no país a partir da Constituição Federal de 1988 (artigo 227); do Estatuto da Criança e do Adolescente (ECA), Lei 8.069/1990, e do Decreto 99.710/1990; da Lei 8.080/1990 do SUS; do Código Civil (CC), Lei 10.104/2002 e da Lei 13.431/2017 (sistema de garantia de direitos da criança e adolescente vítima ou testemunha de violência) e do Decreto 9.603/2018, entre outras normas.

Os textos legais mencionados partem do princípio da proteção, primando o princípio do melhor interesse de crianças e adolescentes e a proteção de seus direitos fundamentais e de personalidade. O ECA, artigo 3º, estabelece a proteção aos direitos da personalidade e fundamentais à garantia a integridade física, moral e psicológica; direitos estes reforçados pelo Código Civil, em seu Capítulo II, dos artigos 11 ao 21.

E na outra ponta, o sistema busca desestimular práticas ilícitas, imorais e vergonhosas de abuso de crianças e adolescentes, os números oficialmente registrados são significativos, mas sabemos que a subnotificação é uma realidade nefasta.[229]

> "Embora o número total de nascidos-vivos no Brasil, venha diminuindo lentamente com o passar dos anos, percebe-se um aumento na taxa de fecundidade de mães de 10-13 anos. Em 2015 nasceram 5.828 bebês, filhos de mães dessas idades. Apesar das regiões Centro-Oeste e Sudeste expressarem redução da taxa de fecundidade na faixa etária de 10-13 anos, houve aumento nas regiões Norte, Nordeste e Sul do Brasil (SINASC, 2015). Dados de 2017 da proporção de nascidos vivos de mães com idade entre 10 e 19 anos, evidenciam diferenças regionais, com a média nacional de 16,4%, sendo 23,7% na região Norte,

[229] SCHUMACHER GS, GARCIA LF, FERNANDES MS, GOLDIM JR. Violência contra crianças na perspectiva de profissionais de saúde: reconhecimento e proteção em suas atividades hospitalares. Rev Bio y Der. 2018; 44: 149-62.

> 19,9% na região Nordeste, 15,4% na região Centro-Oeste, 13,3% na região Sudeste e 13,1% na região Sul. Cerca de 24.000 nascimentos são de mães na faixa de 10 a 14 anos.[230]

Neste sentido, destacam-se a Portaria 1.968/2001 do Ministério da Saúde (notificação de maus-tratos); a Lei 13.431/2017, que dispõe sobre o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência que trata; que é regulada pelo Conselho Nacional de Justiça, por meio da Resolução No 299 de 05 de novembro de 2019 e a Lei Geral de Proteção de Dados, Lei 13.709/2018, com previsão expressa a proteção do tratamento de dados de crianças e adolescentes, no seu artigo 14.

Em particular, as regras gerais de incapacidade civil, previstas no Código Civil (CC), Lei 10.104/2002, artigos 3º e 4º, que estabelecem os critérios para a incapacidade absoluta e a incapacidade relativa, foram limitadas pelas alterações dos incisos I, II e III do artigo 3º e incisos II e III e paragrafo único do artigo 4º do CC impostos pelo artigo 114, do Estatuto da Pessoa com Deficiência (EPD), Lei 13.146/2015, para atingir outras situações de incapacidade, além do critério fático da idade biológica. Cabe destacar o motivo de nossa critica, que já tivemos a oportunidade de tratar mais detidamente em outro trabalho. A critica ao EPD não diz respeito ao necessário reconhecimento legal e social à igualdade de direitos civis, especialmente e, acima de tudo, a igualdade de oportunidades as pessoas com deficiência – física e/ou psicológica; mas sim nossa crítica diz respeito a supressão do critério do "necessário discernimento" como suporte fático dos artigos 3º e 4º do CC, que era a porta normativa para promover a proteção inúmeros casos de pessoas com deficiência mental, nos seus diferentes graus.

Estas alterações, em nosso entender, estão na contra mão dos princípios da operabilidade, eticidade e socialidade[231], pilares do CC, concebidos por Miguel Reale justamente para possibilitar novas formas de interpretação jurídica. Na realidade as mudanças promoveram uma situação de insegurança jurídica, especialmente para os deficientes mentais ou pessoas sem necessário discernimento, por causa permanente ou transitória, que não possam exprimir, declarar ou manifestar a sua vontade e o seu consentimento. Vejamos alguns exemplos que sustentam nosso ponto, os efeitos do artigo 166, inciso I, que determina a nulidade dos negócios jurídicos celebrados por absolutamente incapaz, restringido o suporte fático da norma ao critério de idade, menores de 16 anos (artigo 3º, Caput) e não mais as pessoas "sem o necessário discernimento"; fato que também ocorre com os efeitos da imprescritibilidade, artigo 198, inciso I, do CC que antes do EPD atingia as pessoas elencadas nos revogados incisos I, II e III do artigo 3º do CC, isso é "pessoas sem o necessário discernimento".

Miguel Reale, quando da elaboração do Projeto do Código Civil Brasileiro, hoje CC, adotou o modelo biopsicológico para pautar a Teoria das Incapacidades, justifi-

---

[230] CUNHA, Ana. Direitos sexuais e reprodutivos dos adolescentes. Revista FEMINA, 2020, 48(2):70-81. Publicação oficial da Federação Brasileira das Associações de Ginecologia e Obstetrícia. Acessível em https://www.febrasgo.org.br/media/k2/attachments/FEMINAZ2.pdf

[231] MARTINS-COSTA, Judith e BRANCO, Gerson. Diretrizes Teóricas do Novo Código Civil Brasileiro. São Paulo: Editora Saraiva, 2002.

cando que este modelo jurídico, por estar alicerçado nos "melhores subsídios da Psiquiatria e da Psicologia, atingiria os diferentes estágios de desenvolvimento psicológico moral e as avaliações das condições de discernimento mental dos indivíduos, em respeito a heterogeneidade dos seres humanos, conectados a vida real.[232]

O núcleo semântico da palavra "discernimento", como coloca Judith Martins-Costa no contexto normativo do CC, é onde residia os elementos do "conceito de capacidade para consentir"[233]. Conceito este tão caro para justificar a participação ativa de crianças e adolescentes no processo de consentimento na área da saúde, para tomada de decisão em seu melhor interesse; assim como o era para permitir que pessoas com capacidade legal, mas que não dispunham da capacidade emocional pudessem ser protegidas.

Martins-Costa, destaca quatro momentos centrais do conceito de "capacidade de consentir", com base na obra de André Gonçalo Dias Pereira. São eles: 1) a capacidade de decidir sobre valores, com ponderação de custos e benefícios; 2) a capacidade para apreciar os fatos; 3) a capacidade para entender as alternativas e 4) a capacidade para se autodeterminar com base nas informações recebidas.[234]

2. Os elementos extrínsecos do Processo de Consentimento

Por sua vez, os elementos extrínsecos do processo de consentimento informado, conectam-se às condições concretas, fáticas e situacionais de quem consente, considerando a forma, o modo e o lugar que o processo de consentimento se apresenta.

O processo de consentimento na área da saúde deve ser orientador, tanto na pesquisa envolvendo seres humanos, como na assistência à saúde. O modo que o processo deve ser aplicado deve considerar o perfil dos profissionais de saúde que são os emissores das informações que fundamentam o consentimento. Quanto ao aspecto ambiental, o local deve ser amigável, acolhedor e com respeito aos direitos à privacidade e à confidencialidade, imagem e proteção de dados pessoais.

O Termo de Consentimento, que serve de documentação para o processo, deve ser legível, compreensível e ter a sua finalidade claramente apresentada. Ser legível é ter o cuidado com a sua redação adequada, tanto em termos de estrutura quanto de vocabulário utilizado. Ser compreensível é garantir que a pessoa que irá ler o documento tenha o adequado entendimento do que está sendo apresentado, de quem são as pessoas e instituições envolvidas, do que será feito, das garantias, dos direitos e dos deveres

---

232 REALE, Miguel. História do novo Código Civil. São Paulo: Revista dos Tribunais, 2005.

233 MARTINS-COSTA, Judith. Capacidade para consentir e esterilização de mulheres tornadas incapazes pelo uso de drogas: notas para uma aproximação entre a técnica jurídica e a reflexão bioética. In: Judith Martins-Costa; Letícia Ludwing Möller (Org.). Bioética e responsabilidade. Rio de Janeiro: Forense, 2009.

234 MARTINS-COSTA, Judith. Capacidade para consentir e esterilização de mulheres tornadas incapazes pelo uso de drogas: notas para uma aproximação entre a técnica jurídica e a reflexão bioética. In: Judith Martins-Costa; Letícia Ludwing Möller (Org.). Bioética e responsabilidade. Rio de Janeiro: Forense, 2009; p. 326.

associados. Neste documento devem constar os riscos, desconfortos e benefícios associados. É fundamental que o documento apresente claramente o que é que está sendo proposto, seja um procedimento assistencial ou um projeto de pesquisa.[235]

Os elementos extrínsecos, também devem englobar, o que Judith Martins-Costa denomina como "assistência coletiva e dialogal", pois resultará de um processo em que a convicção se forma por meio da conjunção de elementos técnicos, sociais e psicológicos"[236].

Nesta mesma linha, na perspectiva da Bioética e do Biodireito, a análise da "capacidade para consentir" de crianças e adolescentes deve ser analisado por meio de uma perspectiva integrada, não excludente, dos princípios da dignidade, autonomia, vulnerabilidade e integridade. Os quatro princípios - dignidade, autonomia, vulnerabilidade e integridade, articulados por Kemp e Rendtorff[237], devem ser interpretados de forma integrada, considerando expressões da realidade fenomenológica concreta do cotidiano da vida humana, no âmbito da solidariedade e responsabilidade. Resumidamente demarcam estes princípios da seguinte forma:

A dignidade não deve se restringir a autonomia, mas deve ser destacada como o valor fundante e intrínseco do indivíduo de todo ser humano em seu encontro com o outro. A dignidade diz respeito a si e aos outros: devo me comportar com dignidade e devo considerar a dignidade do outro; ou seja não devo abandonar o comportamento civilizado e responsável.

A autonomia não deve ser apenas interpretada no sentido liberal de "permissão", mas sim deve-se considerar cinco aspectos da autonomia: 1) a capacidade de criação de ideias e objetivos para a vida; 2) a capacidade de inserção moral, autocontrole e privacidade; 3) capacidade de decisão e ação racionais sem coerção; 4) capacidade de envolvimento político e responsabilidade pessoal; 5) capacidade de consentimento informado.

A vulnerabilidade, por sua vez, diz respeito à integridade como um princípio básico para o respeito e a proteção da vida humana e não humana. O princípio da vulnerabilidade pode estabelecer pontes entre estranhos morais em uma sociedade pluralista. Da mesma forma, reconhecer a vulnerabilidade deve ser um dos pontos de partida essencial para a formulação de políticas no moderno estado de bem-estar social. O respeito à vulnerabilidade não é uma demanda por vida perfeita e imortal, mas o reconhecimento da finitude da vida e, em particular, a presença terrena de sofrimento dos seres humanos.[238]

---

[235] Goldim, J. R. O consentimento informado e a adequação de seu uso na pesquisa em seres humanos. Tese (Doutorado em Medicina) - Faculdade de Medicina, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1999.

[236] MARTINS-COSTA, Judith. Capacidade para consentir e esterilização de mulheres tornadas incapazes pelo uso de drogas: notas para uma aproximação entre a técnica jurídica e a reflexão bioética. In: Judith Martins-Costa; Letícia Ludwing Möller (Org.). Bioética e responsabilidade . Rio de Janeiro: Forense, 2009; p. 339.

[237] FERNANDES, Márcia S. Implicações Éticas e Legais no atendimento de pacientes menores de 14 anos. Revista FEMINA, 2020, 48(2):70-81. Publicação oficial da Federação Brasileira das Associações de Ginecologia e Obstetrícia. Acessível em https://www.febrasgo.org.br/media/k2/attachments/FEMINAZ2.pdf

[238] GUIMARÃES MCS, NOVAES SC. Autonomia reduzida e vulnerabilidade: liberdade de decisão, diferença e desigualdade. Rev Bioética. 1999;7(1):1–3.

A integridade está conectada com a retidão, honestidade e boas intenções, a integridade é considerada universalmente como uma qualidade da pessoa como tal. Assim, refere-se à coerência da vida no tempo e no espaço (na memória e na vida corporal) que não deve ser tocada e destruída. É a coerência da vida, que é lembrada a partir de experiências e, portanto, pode ser contada em uma narrativa. Assim, o respeito à integridade é o respeito à privacidade e ao ambiente pessoal e, em particular, ao entendimento do paciente sobre sua própria vida e doença no corpo e na alma. A integridade é o princípio mais importante para a criação de confiança entre o médico e o paciente, porque exige que o médico ouça o paciente contando a história sobre sua vida e doença.[239]

3.Consentimento, Assentimento e Autorização por Representação

Muitos documentos regulatórios relacionados à pesquisa envolvendo seres humanos têm utilizado a denominação de "assentimento" para se referir ao consentimento dado por crianças e adolescentes. A crítica à utilização deste termo não é recente[240]. Um importante questionamento se refere ao próprio significado de assentimento, que remete a aceitar, a anuência, a concordar ou aprovar uma proposta feita.[241]

O processo de consentimento pressupõe a liberdade de poder optar entre as alternativas existentes em uma situação. Um convite para participar de uma pesquisa ou a proposta de realização de um procedimento assistencial implica na possibilidade da pessoa poder concordar ou discordar com a sua realização. Se for utilizada a denominação de assentimento, o processo de tomada de decisão passa a envolver apenas uma alternativa: aceitar a proposta. É uma maneira de incluir os menores no processo de tomada de decisão, mas partindo do pressuposto de que eles irão aceitar a proposta apresentada. Independentemente da idade, desde que haja um desenvolvimento psicológico-moral compatível, é fundamental garantir a liberdade de escolha, ou seja, de poder optar entre as diferentes alternativas existentes.[242]

É fundamental discutir o papel das crianças, adolescentes e da família na obtenção do consentimento. A maioria dos textos legais transfere para os pais, tutores ou curadores o poder de decisão sobre a participação ou não de seus filhos menores de idade em projetos de pesquisa ou na realização de procedimentos assistenciais. Os pais, ou

---

[239] FERNANDES, Márcia S. Implicações Éticas e Legais no atendimento de pacientes menores de 14 anos. Revista FEMINA, 2020, 48(2):70-81. Publicação oficial da Federação Brasileira das Associações de Ginecologia e Obstetrícia. Acessível em https://www.febrasgo.org.br/media/k2/attachments/FEMINAZ2.pdf

[240] BAZZANO LA, DURANT J, BRANTLEY PR. A modern history of informed consent and the role of key information. Ochsner J. 2021;21(1):81–5.

[241] GRIGOLO, R.; FERNANDES, MÁRCIA S.; GOLDIM J.R. AUTONOMIA, AUTODETERMINAÇÃO E INCAPACIDADE CIVIL: UMA ANÁLISE SOB A PERSPECTIVA DA BIOÉTICA E DOS DIREITOS HUMANOS'. REVISTA DE DIREITOS E GARANTIAS FUNDAMENTAIS (FDV), v.18, p.239 - 266, 2017. Acessível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1128

[242] Goldim, J. R. O consentimento informado numa perspectiva além da autonomia. Revista da Amrigs, Porto Alegre, v. 46, n. 3-4, p.109-116, jul./dez. 2002.

outros representantes legais, assumem o processo de tomada de decisão e de consentimento.[243]

Desde o ponto de vista ético, o consentimento é um ato personalíssimo, ou seja, apenas a própria pessoa pode manifestar as suas escolhas, na perspectiva do seu melhor interesse, ou seja, dar o seu consentimento. O chamado consentimento dos pais, a rigor, é uma autorização por representação[244]. Desde o ponto de vista legal, os pais têm a prerrogativa de tomar decisões na perspectiva do melhor interesse de seus filhos. Isto em nada altera a participação dos pais, mas dá uma denominação adequada ao que de fato ocorre – como ressaltamos na Parte I de nosso texto, as palavras estão envoltas por sentidos etimológicos, sociais e culturais.

As crianças e os adolescentes que já têm desenvolvimento psicológico-moral compatível com a tomada de decisão no seu melhor interesse, podem dar o seu consentimento, desde o ponto de vista ético, complementado pela perspectiva legal da autorização e emocionalmente "apoiada" por representação de seus pais ou tutores. Aqui, o conceito de "tomada de decisão apoiada", prevista no artigo 1.783-A do CC, introduzido pela Lei 13.146/2015, artigo 116, poderia fazer sentido, entretanto assim não poderá, pois o seu suporte fático está restrito a pessoa com deficiência.

O processo de tomada de decisão familiar é caracterizado pela conjugação do consentimento do menor com a autorização por representação de seus responsáveis. Esta proposta garante a participação ativa, tanto da criança ou adolescente, quanto de seus pais ou representantes. Esta é a melhor estratégia de abordagem do processo de consentimento em menores de idade, pois permite resguardar os aspectos éticos e legais associados. Desde o ponto de vista de documentação, poderia ser elaborado um Termo de Consentimento, onde constasse o consentimento em si do menor e, no mesmo instrumento, a autorização por representação de seus responsáveis. Este documento, que contém as informações essenciais necessárias ao adequado esclarecimento das alternativas propostas, registra o processo de decisão familiar realizado de forma conjunta.

4. O Processo de Consentimento nas pesquisas clínicas envolvendo crianças e adolescentes

Além das questões éticas e legais associadas ao ato de consentir, o processo de consentimento também envolve outras questões importantes, como a própria justificativa para a realização de pesquisas em crianças e adolescentes. [245]

---

[243] RAYMUNDO, Márcia M. e GOLDIM, J.R. Moral-psychological development related to the capacity of adolescents and elderly patients to consent. J Med Ethics 2008;34:602–605. doi:10.1136/jme.2007.022111. Downloaded from http://jme.bmj.com/ on June 13, 2015.

[244] RAYMUNDO MM, GOLDIM JR. Do consentimento por procuração à autorização por representação. Bioética [Internet]. 2007;15(1):83–99. Acessível em: http://www.portalmedico.org.br/bioetica/edicoes/2007/15-1/revista.pdf

[245] KIPPER DJ, GOLDIM JR. A pesquisa em crianças e adolescentes. J Pediatr (Rio J). 1999;75(4):211–2.

Muitas vezes, com a intenção de proteger pessoas tidas como vulneráveis, os documentos regulatórios de pesquisa em seres humanos, ao longo do tempo, excluíram grupos de pessoas, como crianças, adolescentes, idosos, gestantes, doentes mentais e prisioneiros, por exemplo.

A proteção por exclusão se justifica pela exposição pontual, mas gera uma vulnerabilidade ainda maior posterior. A falta de pesquisas gera insegurança às atividades assistenciais. Foi constatado, em diferentes países, que uma grande parte das medicações utilizadas em crianças e adolescentes não tinham qualquer estudo que embasasse a sua utilização, as doses e esquemas terapêuticos utilizados. O uso off label de medicamentos é realizado com base na transposição dos resultados obtidos em pessoas adultas. As características biológicas próprias da infância e da adolescência dificultam esta simples transposição de esquemas terapêuticos[246].

Com base nestas constatações, foi novamente incentivada a realização de pesquisas clínicas em crianças e adolescentes. O importante é que estes projetos tivessem como plano de fundo o melhor interesse das crianças e adolescentes e a geração de conhecimentos voltados a esta faixa etária. As atividades de pesquisa clínica envolvem maior controle e monitoramento do que as realizadas assistencialmente. Existe um balanço adequado do benefício individual e coletivo associado a um controle de riscos individuais de cada participante.

As pesquisas que podem ser realizadas em outras faixas etárias devem preceder as desenvolvidas em crianças e adolescentes. Desta forma, existirão dados de segurança que poderão ser melhor avaliados antes da sua realização com estes grupos. O desenvolvimento das vacinas para a COVID-19, é um bom exemplo desta prática. Foram realizados inúmeros projetos com o envolvimento de diferentes grupos de pessoas, em termos de idade, sexo, condições de saúde e de estilo de vida, antes de sua utilização em crianças e adolescentes.

A realização de tratamentos assistenciais tem como característica básica a necessidade associada. Uma vez constatada a alternativa, ela é apresentada ao paciente e aos seus responsáveis como sendo necessária, desde o ponto de vista assistencial. Esta é a convicção da equipe assistencial.

Nas situações envolvendo doenças raras, a necessidade de realização de pesquisas clínicas é ainda maior. Muitas vezes a única chance de ter alguma possibilidade de tratamento é durante a realização de uma pesquisa clinica.

Nas pesquisas clínicas existe a sobreposição destas duas situações anteriores, ou seja, existe uma necessidade na perspectiva do paciente que é associada à possibilidade de vir a ser um participante de pesquisa. Esta é uma situação onde necessidade e possibilidade se conjugam, pode ser caracterizada como sendo uma contingência.

Na contingência associada à pesquisa clínica, a liberdade do menor e de seus representantes de poder tomar decisões deve ser garantida, mas a equipe de pesquisa,

---

246 FERREIRA L DE A, IBIAPINA C DA C, MACHADO MGP, FAGUNDES EDT. A alta prevalência de prescrições de medicamentos off-label e não licenciados em unidade de terapia intensiva pediátrica brasileira. Rev Assoc Med Bras. 2012;58(1):82–7.

que assume também um papel assistencial, pode enfatizar a necessidade de saúde associada. São situações delicadas de conduzir, que devem sempre ter como objetivo fundamental a busca do melhor interesse da criança ou do adolescente.

Por outro lado, a participação em pesquisa não clínica deve ser sempre apenas uma possibilidade, nunca uma necessidade. A criança ou adolescente pode ser convidado a participar de um projeto de pesquisa, que não envolva situações assistenciais, e deve ter a garantia da sua liberdade de poder aceitar ou não este convite. As crianças e adolescentes são detentores da "capacidade de consentir", integrante da "capacidade de Direito", que abrange a ampla perspectiva existencial dos seres humanos, ainda que sejam absolutamente ou relativamente incapazes juridicamente. Em pesquisas não clínicas a participação das crianças e adolescentes no processo de consentimento é essencial.

5. O Processo de Consentimento e a assistência à saúde de crianças e adolescentes

Na assistência às crianças e adolescentes a relação dos profissionais de saúde envolve os pacientes e seus pais, ou outros representantes legais. Na maioria das vezes é uma relação que ocorre entre várias pessoas e não apenas entre um profissional e um paciente.

Na medida em que as crianças vão se desenvolvendo, a sua participação também se torna progressivamente crescente e ativa no processo assistencial. Os profissionais devem sempre atentar para a capacidade de compreensão das crianças sobre os procedimentos assistenciais que serão com elas realizados, direito também garantido pelo ECA.[247]

Portanto, explicar, previamente, ao paciente (criança ou adolescente) o que será feito é sempre importante. Não surpreender é garantir a preservação da relação de confiança. Na medida em que a criança se desenvolve, é fundamental envolve-la nos processos de tomada de decisão. Por exemplo, informar que será realizado um simples exame físico e pedir a sua autorização para retirar uma roupa, informar que o seu corpo será tocado e explicar o que será feito é fazer um processo de consentimento.

Nas situações assistenciais algumas vezes é necessário ter uma postura de proteção ativa, quando a necessidade se impõe, quando a realização de um procedimento se torna imperiosa a ponto de garantir a sobrevida do paciente. Nestas situações, caracterizadas como de emergência, o bem do paciente se impõe à sua autonomia e a sua autodeterminação.

Os adolescentes já podem ter situações que demandem uma maior proteção à sua privacidade. Existem situações assistenciais onde um paciente solicita ao seu médico que não compartilhe informações com seus pais. O Código de Ética Médica, de 2018, estabelece que o médico deve cumprir com o seu dever de proteger a privacidade do

[247] Os direitos da personalidade, em particular os direitos à privacidade, dos pacientes menores de 14 anos está devidamente protegida pelo Estatuto da Criança e Adolescentes, conforme previsto no artigo 17, que determina que "o direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais."

paciente menor de idade, desde que julgue que o paciente tem condições de lidar adequadamente com a situação que está sendo objeto de assistência.[248] Todos os registros assistenciais e esta solicitação de não compartilhamento de informações devem ser documentados em prontuário. Caso os pais ou representantes legais solicitem estas informações diretamente ao médico, especificamente sobre esta situação, ele deverá resguardar o paciente.

Em algumas situações assistenciais extremas, as equipes assistenciais podem se deparar com pais ou responsáveis legais que, ao seu juízo, tomam decisões não razoáveis, que não atendem aos melhores interesses dos pacientes. Nestes casos pode ser feita a solicitação, por meio do Ministério Público da Infância e da Adolescência, de uma avaliação desta situação onde ocorreu uma negativa ao consentimento para a realização de um procedimento tido como mandatório pela equipe assistencial. São situações extremas, que justificam a existência de estruturas sociais de proteção aos menores. [249]

6. O Processo de Consentimento na LGPD e o tratamento de dados pessoais de crianças e adolescentes

A Lei Geral de Proteção de Dados, Lei 13.709/2018, tem o objetivo de proteger e garantir aos titulares de dados pessoais e dados pessoais sensíveis o tratamento adequado, lícito e em respeito a sua privacidade. A Emenda Constitucional 115, elevou esta proteção à categoria de direito fundamental, incluindo ao artigo 5º, inciso LXXIX, da Constituição Federal.

A LGPD deve tratar dados pessoais pautada pelos princípios, previstos no artigo 6º da Lei. Portanto, a adequação a finalidade, necessidade, adequação e a boa-fé objetiva, dentre outros princípios, prevê o consentimento informado do titular dentre bases legais para tratamento de dados pessoais, artigo 8º, da LGPD. No caso de crianças e adolescentes, o princípio do melhor interesse das crianças e adolescentes se sobrepõe é central para análise do artigo 14 §1° e o tratamento de dados deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Assim, a natureza jurídica, a finalidade e a forma do processo de consentimento informado na LGPD, conforme já tivemos oportunidade de mencionar na Parte I e II deste texto, é distinta dos processos de consentimento necessários para a realização de pesquisas envolvendo seres humanos ou mesmo para a assistência à saúde. E no caso de tratamento de dados de crianças e adolescentes estas diferenças também se mantém.

O consentimento na LGPD, é um ato jurídico stricto sensu e sua forma, finalidade e efeitos estão previamente previstos no artigo 8º da LGPD, como uma das bases legitimas de tratamento de dados pessoais e dados pessoais sensíveis, portanto os seus efeitos estão circunscritos a autorização do titular ou de seu representante legal para o tratamento

---

[248] O sigilo profissional é assegurado pelo Capítulo IX do Art. 74 do CEM/2018: "É vedado ao médico revelar sigilo profissional relacionado à paciente criança ou adolescente, desde que estes tenham capacidade de discernimento, inclusive a seus pais ou representantes legais, salvo quando a não revelação possa acarretar dano ao paciente".

[249] RHODES R, HOLZMAN IR. Is the best interest standard good for pediatrics? Pediatrics. 2014 Oct [cited 2015 Jan 15];134 Suppl(October):S121-9.

de dados e informações pessoais, em respeito aos seus direitos de personalidade e ao princípio da autodeterminação informativa.

Assim, nos casos de pesquisa clinica envolvendo crianças e adolescentes, o tratamento de dados pessoais (artigo 5º, inciso X) se mantém semelhantes as demais situações, com adultos; observando, impreterivelmente, a atenção e respeito ao princípio do melhor interesse da criança e do adolescente (artigo 14).[250]

Outrossim, o tratamento de dados pessoais e dados pessoais sensíveis de crianças e adolescentes poderão ser realizados em situações de pesquisas, desde que realizadas por órgão de pesquisa, artigo 5º, inciso XVIII e artigo 13 e parágrafos, para a realização de "estudos em saúde pública".

A dispensa do consentimento específico da LGPD, art. 8º, quando outras bases legais legitimarem o tratamento de dados pessoais e sensíveis, previstos nos artigos 7º, IV, VII e 11, II, letra "a" e "e", quando devidamente justificado pelas circunstâncias, atingem em nosso entender também os dados pessoais de crianças e adolescentes.

A dispensa do consentimento no caso de pesquisas pela LGPD, não altera as responsabilidades inerentes aos promotores e responsáveis pela pesquisa clínica (sejam patrocinadores, instituições envolvidas e pesquisadores responsáveis) em promover ambiente seguro para o tratamento de dados pessoais e dados pessoais sensíveis relacionados aos participantes no desenvolvimento da pesquisa. Este ambiente seguro deve ser de responsabilidade do controlador ou controladores, que no caso das pesquisas clinicas são os pesquisadores e demais responsáveis pela pesquisa, posição que se impõe indiscutivelmente no caso dos dados pessoais de crianças e adolescentes.

O desenho do projeto de pesquisa e o contrato de pesquisa, devem prever a definição das obrigações e de medidas de segurança concretas, conforme exigidas pela LGPD para o tratamento dos dados pessoais dos participantes de pesquisa sejam pessoas adultas ou crianças e adolescentes; com a devida apreciação e aprovação de Comitê de Ética em Pesquisa (CEP). Ainda, devem ser estabelecidos controles e mecanismos para auditar as bases de dados e, sempre que possível, utilizar a pseudonimização ou outras técnicas de proteção dos dados de pesquisa que oriundos de dados e informações pessoais dos participantes, em vista do princípio de seu melhor interesse.

No caso da pesquisa envolvendo crianças e adolescentes, os responsáveis da pesquisa, como controladores e/ou controladores conjuntos, devem elaborar e desenhar o projeto de pesquisa clinica com metodologia adequada, contendo formas de tratamento e governança dos dados pessoais dos participantes para garantir a sua autodeterminação, inclusive para garantir a retirada do consentimento do participante e de seu representante legal, com o dobro de cuidado com as finalidades, formas e o adequado armazenamento e compartilhamento e descarte dos dados.

Na assistência à saúde, para tratar dados pessoais de saúde de crianças e adolescentes, consentimento da LGPD poderá ser dispensado para realização de assistência, proteger a integridade física e/ou de saúde do titular ou mesmo tratar o dado do titular

[250] SARLET, GABRIELLE B. S.; FERNANDES, MÁRCIA S.; RUARO, REGINA L. A proteção de dados no setor da saúde em face do sistema normativo brasileiro atual in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

em situações de pesquisa.251 E neste caso o controlador – que será o profissional liberal e/ou instituição responsável pela prestação do serviço, as práticas de segurança devem estar previstas em regulamento específico, a forma e o sistema de anotações em prontuário eletrônicos devem ser destacadas nestes casos.

No entanto, a dispensa do consentimento do art. 14§1º da LGPD que falamos nas condições de assistência à saúde de crianças e adolescentes, não dispensa o processo de consentimento para à assistência em si ou para a realização de pesquisas clínicas envolvendo este grupo. O que poderá corre e talvez seja o mais indicado, em termos práticos, é que haja um duplo processo de consentimento no tratamento de dados de crianças e adolescentes, um para assistência e/ou pesquisa e o outro para o tratamento de dados pessoais na forma exigida pela LGPD.

Ressaltamos, no entanto, que dispensar o consentimento para tratamento de dados pessoais, nas situações previstas pela LGPD, não implica em ignorar os seus princípios e regras de direitos, em particular os princípios (artigo 6º) e os direitos dos titulares (dos artigos 17 ao 22).[252] E o tratamento de dados pessoais de crianças e adolescentes, sempre deve ser visando o seu melhor interesse (artigo 14) e deve ter o consentimento especifico e em destaque de um dos pais ou responsável legal, considerando elementos intrínsecos e extrínsecos do consentimento (artigo 14, §§ 1º e 6º). Na ausência do consentimento, só podem serem coletados dados em situações de urgência, devendo-se imediatamente entrar em contato com os pais ou com os responsáveis para garantir a maior e mais adequada proteção à criança e ao adolescente (artigo 14, §3º).[253]

7. Síntese conclusiva da Parte III

As crianças e adolescentes devem ter todos os seus direitos reconhecidos e protegidos nas situações assistenciais e de pesquisa. A efetiva participação nos processos de tomada de decisão e a garantia da proteção à sua privacidade e aos seus dados pessoais sensíveis são imperiosas.

Mais do que um simples processo de consentimento, a proposta de utilização de um processo de tomada de decisão familiar garante participação conjunta das crianças e adolescentes com seus pais, ou representantes legais, na assistência e na pesquisa. As crianças e os adolescentes devem ter a garantia de que serão adequadamente informadas e, na medida de seu desenvolvimento psicológico-moral, de que serão ouvidas e que poderão participar ativa e livremente nas escolhas que serão tomadas. A liberdade

---

251 BARRETO, Mauricio L.; ALMEIDA, Bethânia; DONEDA, Danilo. Uso e proteção de dados pessoais na pesquisa científica, in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

252 SARLET, Gabrielle B. S.; RUARO, Regina L.. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob enfoque da Lei Geral de Proteção de Dados(LGPD), Lei 13.709/2018. in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021.

253 HENRIQUES, IASABELLA; PITA, MARINA E HARTUNG, PEDRO. A proteção de dados pessoais de crianças e adolescentes, in Tratado de Proteção de Dados Pessoais, Coord. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio, Rio de Janeiro: Editora Forense, 2021, p. 199.

para poder tomar decisões, livre de coerção e com o necessário desenvolvimento psicológico-moral, é fundamental.

O marco regulatório e legal, em particular a LGPD, não impede a participação de crianças e adolescentes em projetos de pesquisa, nem a utilização de suas informações. O que deve ser sempre objeto de preocupação dos pesquisadores e órgãos responsáveis pela realização ou regulação de pesquisas em seres humanos, é a garantia da adequação de todas as propostas e ações realizadas, desde o planejamento e avaliação do projeto até a divulgação dos seus resultados. Da mesma forma, os cuidados e salvaguardas devem ser especificamente estabelecidos para a disponibilização, o compartilhamento e o uso para pesquisa, ou outra forma de tratamento de dados pessoais e dados pessoais sensíveis de crianças e adolescentes registrados em prontuário de saúde, físico ou eletrônico.

Síntese geral

O ato de consentir deve ser reconhecido e examinado em cada uma das situações empregadas, para que a "concha a do marisco abondonado" recepcione as características jurídicas adequadas, considerando a diversidade das situações para proteger e garantir ao participante de pesquisa o respeito aos seus direitos.

III_Legislação e Jurisprudência Comentadas

Comentário ao Acórdão do Tribunal de Justiça, de 5 de abril de 2022, proferido no âmbito do Processo C-140/20

Rita Girão Curro[254]

1. Apresentação do Acórdão

Em 5 de abril de 2022, o Tribunal de Justiça ("TJ") pronunciou-se, no âmbito do Processo C-140/20, relativamente (i) à conservação generalizada, seletiva e rápida de dados para efeitos de luta contra a criminalidade grave, (ii) ao acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas e, por fim, (iii) ao alcance e aos efeitos no tempo de uma eventual declaração de não conformidade de uma legislação nacional com o Direito da União Europeia.

2. A questão controvertida

O Processo C-140/20 tem por objeto um pedido de decisão prejudicial apresentado pela *Supreme Court* da Irlanda ao TJ e que incidia sobre a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas ("Diretiva 2002/58/CE"), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 ("Diretiva 2009/136/CE"), lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia ("Carta").

As questões prejudiciais foram colocadas no contexto de um litígio que opôs G.D. ao Commissioner of An Garda Síochána, ao Minister for Communications, Energy and Natural Resources e ao Attorney General, a propósito da validade da Communications (Retention of Data) Act 2011 ("Lei de 2011"), que regulava a conservação de dados de tráfego e dados de localização relativos a chamadas telefónicas, e com base nos quais G.D. foi condenado a uma pena de prisão perpétua pelo crime de homicídio.

---

254 Assistente Convidada da Faculdade de Direito da Universidade de Lisboa. Investigadora do Centro de Investigação de Direito Público da Faculdade de Direito da Universidade de Lisboa. Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa. Pós-Graduada em Teoria e Prática de Contencioso Administrativo e Tributário, Módulo de Contencioso Administrativo, pela Faculdade de Direito da Universidade de Lisboa. Conclusão, na mesma Faculdade, da Parte Curricular do Mestrado em Direito e Ciência Jurídica, Especialidade de Direito Administrativo, estando a desenvolver uma tese em Direito Administrativo.

Segundo G.D., a Lei de 2011 violava os direitos que lhe são conferidos pelo Direito da União Europeia.

Nesse sentido, G.D. instaurou, na *High Court*, uma ação cível com vista à obtenção de uma declaração de invalidade de determinadas disposições da Lei de 2011, que julgou, em 6 de dezembro de 2018, procedente a argumentação de G.D., considerando que o artigo 6.º, n.º 1, alínea a), da Lei de 2011, era incompatível com o disposto no artigo 15.º, n.º 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta.

Por conseguinte, a Irlanda recorreu dessa decisão para a *Supreme Court*, o órgão jurisdicional de reenvio no caso em análise.

Neste âmbito, o órgão jurisdicional de reenvio interrogou-se sobre (i) os requisitos do Direito da União Europeia no que concerne à conservação de dados para efeitos de luta contra a criminalidade grave, (ii) o acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas e, por último, (iii) o alcance e os efeitos no tempo de uma eventual declaração de não conformidade de uma legislação nacional com o Direito da União Europeia.

3. A decisão do Tribunal de Justiça

O TJ, após a apresentação da situação de facto controvertida e do respetivo enquadramento jurídico, analisou as questões prejudiciais submetidas à sua consideração e concluiu o seguinte:

(i) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública;

(ii) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, e desde que essas medidas assegurem, através de regras claras e precisas, que a conservação dos dados está sujeita ao respeito das condições materiais e processuais respetivas e que as pessoas em causa disponham de garantias efetivas contra riscos de abuso, (a) uma conservação seletiva de dados de tráfego e de dados de localização, que seja delimitada, (b) uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário, (c) uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicação eletrónicos e, por último, (d) uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que dispõem;

(iii) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas incumbe a um

agente de polícia, assistido por uma unidade instituída no âmbito da polícia, que goza de um certo grau de autonomia e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional e, por fim;

(iv) O Direito da União Europeia deve ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, em razão da incompatibilidade de uma legislação nacional com o artigo 15.º, n.º 1, da Diretiva 2002/58/CE.

4. Comentário

De modo a justificar as conclusões apresentadas acima, nos pontos (i) e (ii), o TJ assenta, principalmente, na jurisprudência decorrente do seu Acórdão de 6 de outubro de 2020, proferido no âmbito dos processos apensos C-511/18, C-512/18 e C-520/18.

Neste sentido, o TJ entendeu, essencialmente, que (i) na interpretação de uma disposição do Direito da União Europeia, há que atender aos seus termos, contexto, objetivos e génese, (ii) a Diretiva 2002/58/CE tem por finalidade proteger os utilizadores dos serviços de comunicações eletrónicas contra os riscos para os seus dados pessoais e a sua vida privada resultantes das novas tecnologias, nomeadamente, da crescente capacidade de armazenamento e de processamento de dados, não se limitando a enquadrar o acesso a esses dados através de garantias destinadas a prevenir abusos, mas, consagrando o princípio da proibição do seu armazenamento por terceiros, o que significa que as medidas legislativas permitidas aos Estados-Membros, ao abrigo do artigo 15.º, n.º 1, não podem justificar que a derrogação da obrigação de garantia da confidencialidade das comunicações eletrónicas e dos respetivos dados se converta em regra geral e (iii) a possibilidade de os Estados-Membros justificarem uma restrição aos direitos e deveres previstos na Diretiva deve ser apreciada através da medição da gravidade da ingerência que tal restrição implica e da verificação de que a importância do objetivo de interesse geral prosseguido por esta restrição está relacionada com essa gravidade. Neste sentido, o TJ acrescentou ainda que (i) a legislação nacional deve prever uma conservação de dados que assente em elementos objetivos e não discriminatórios e (ii) é aos Estados-Membros (e não ao TJ) que compete a identificação desses critérios, sendo que a dificuldade dessa identificação não pode justificar que os Estados-Membros, fazendo da exceção a regra, prevejam uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização.

De seguida, e com um caráter mais inovador, o TJ clarificou que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas incumbe a um agente de polícia, assistido por uma unidade instituída no âmbito da polícia, que goza de um certo grau de autonomia

e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional. Esta conclusão resulta, desde logo, de duas premissas essenciais: segundo o TJ, o respeito pelas condições materiais e processuais que regem o acesso das autoridades aos dados e a sua utilização exige (i) que esse acesso esteja sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente e (ii) que a decisão desse órgão jurisdicional ou dessa entidade administrativa independente seja tomada na sequência de um pedido fundamentado dessas autoridades, apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal.

No caso em concreto, a Lei de 2011 atribuía a um agente de polícia a competência para exercer o controlo prévio dos pedidos de acesso aos dados que emanavam dos serviços de investigação policial e para solicitar aos prestadores de serviços de comunicações eletrónicas que lhe comunicassem os dados por eles conservados. Consequentemente, o TJ considerou que (i) este agente, não tendo a qualidade de terceiro em relação a esses serviços, não cumpria as exigências de independência e de imparcialidade, ainda que fosse assistido por uma unidade da polícia que beneficiasse de um certo grau de autonomia no exercício da sua missão e (ii) uma fiscalização posterior da decisão do agente de polícia competente, através de uma reclamação ou de um processo judicial destinado a verificar a aplicação das disposições da Lei de 2011, não poderia substituir a exigência de um controlo prévio.

Por fim, recordando o princípio do primado do Direito da União Europeia, o TJ entendeu que o Direito da União Europeia deveria ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, em razão da incompatibilidade de uma legislação nacional com o artigo 15.º, n.º 1, da Diretiva 2002/58/CE. Na verdade, segundo o TJ, a manutenção dos efeitos da Lei de 2011 significaria que uma legislação nacional continuaria a impor aos prestadores de serviços de comunicações eletrónicas obrigações contrárias ao Direito da União Europeia, com graves ingerências nos direitos fundamentais das pessoas cujos dados foram conservados.

Como evidenciado pelo Advogado-Geral, este Acórdão reflete a preocupação suscitada nos Estados-Membros pela jurisprudência do TJ relativa à conservação e ao acesso a dados pessoais gerados no âmbito das comunicações eletrónicas, manifestando-se agregador de vasta jurisprudência do TJ nesta matéria (cf., por exemplo, os Acórdãos dos TJ (i) de 6 de outubro de 2020, proferido no âmbito dos processos apensos C-511/18, C-512/18 e C-520/18, (ii) de 8 de abril de 2014, proferido no âmbito dos processos apensos C-293/12 e C-594/12, (iii) de 21 de dezembro de 2016, proferido no âmbito dos processos apensos C-203/15 e C-698/15 e, por último, (iv) de 2 de outubro de 2018, no âmbito do processo C-207/16).

Acórdão do Tribunal de Justiça (Grande Secção), de 5 de abril de 2022, proferido no âmbito do Processo N.º C-140/20

«Reenvio prejudicial – Tratamento de dados pessoais no setor das comunicações eletrónicas – Confidencialidade das comunicações – Prestadores de serviços de comunicações eletrónicas – Conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização – Acesso aos dados conservados – Fiscalização jurisdicional ex post – Diretiva 2002/58/CE – Artigo 15.º, n.º 1 – Carta dos Direitos Fundamentais da União Europeia – Artigos 7.º, 8.º, 11.º e 52.º, n.º 1 – Possibilidade de um órgão jurisdicional nacional limitar no tempo os efeitos de uma declaração de invalidade de uma legislação nacional incompatível com o direito da União – Exclusão»

No processo C-140/20,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pela Supreme Court (Supremo Tribunal, Irlanda), por Decisão de 25 de março de 2020, que deu entrada no Tribunal de Justiça na mesma data, no processo

G.D.
contra
Commissioner of An Garda Síochána,
Minister for Communications, Energy and Natural Resources,
Attorney General,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis e N. Jääskinen, presidentes de secção, T. von Danwitz (relator), M. Safjan, F. Biltgen, P. G. Xuereb, N. Piçarra, L. S. Rossi e A. Kumin, juízes,

advogado-geral: M. Campos Sánchez-Bordona,

secretário: D. Dittert, chefe de unidade,

vistos os autos e após a audiência de 13 de setembro de 2021,

vistas as observações apresentadas:

— em representação de G.D., por J. Dunphy, solicitor, R. Kennedy, R. Farrell, SC, e K. McCormack, BL,

— em representação do Commissioner of An Garda Síochána, do Minister for Communications, Energy and Natural Resources e do Attorney General, por M. Browne, S. Purcell, C. Stone, J. Quaney e A. Joyce, na qualidade de agentes, assistidos por S. Guerin, P. Gallagher, SC, D. Fennelly e L. Dwyer, BL,

— em representação do Governo belga, por P. Cottin e J.-C. Halleux, na qualidade de agentes, assistidos por J. Vanpraet, advocaat,

— em representação do Governo checo, por M. Smolek, O. Serdula e J. Vláčil, na qualidade de agentes,

— em representação do Governo dinamarquês, inicialmente por J. Nymann-Lindegren, M. Jespersen e M. Wolff, e em seguida por M. Wolff e V. Jørgensen, na qualidade de agentes,

— em representação do Governo estónio, por A. Kalbus e M. Kriisa, na qualidade de agentes,

— em representação do Governo espanhol, por L. Aguilera Ruiz, na qualidade de agente,

— em representação do Governo francês, por E. de Moustier, A. Daniel, D. Dubois, T. Stéhelin e J. Illouz, na qualidade de agentes,

— em representação do Governo cipriota, por I. Neophytou, na qualidade de agente,

— em representação do Governo neerlandês, por C. S. Schillemans, K. Bulterman e A. Hanje, na qualidade de agentes,

— em representação do Governo polaco, por B. Majczyna e J. Sawicka, na qualidade de agentes,

— em representação do Governo português, por L. Inez Fernandes, P. Barros da Costa e I. Oliveira, na qualidade de agentes,

— em representação do Governo finlandês, por M. Pere e A. Laine, na qualidade de agentes,

— em representação do Governo sueco, por O. Simonsson, J. Lundberg, H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson e H. Eklinder, na qualidade de agentes,

— em representação da Comissão Europeia, por S. L. Kalėda, H. Kranenborg, M. Wasmeier e F. Wilman, na qualidade de agentes,

— em representação da Autoridade Europeia para a Proteção de Dados, por D. Nardi, N. Stolič, K. Ujazdowski e A. Buchta, na qualidade de agentes, ouvidas as conclusões do advogado-geral na audiência de 18 de novembro de 2021,

profere o presente

Acórdão

1 O pedido de decisão prejudicial tem por objeto a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11) (a seguir «Diretiva 2002/58»), lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

2 Este pedido foi apresentado no âmbito de um litígio que opõe G.D. ao Commissioner of An Garda Síochána (Comissário da Polícia Nacional, Irlanda), ao Minister for Communications, Energy and Natural Resources (Ministro das Comunicações, Energia e Recursos Naturais, Irlanda) e ao Attorney General a respeito da validade do Communications (Retention of Data) Act 2011 [Lei das Comunicações (Conservação de Dados) de 2011, a seguir «Lei de 2011»].

Quadro jurídico

Direito da União

3 Os considerandos 2, 6, 7 e 11 da Diretiva 2002/58 enunciam:

«(2) A presente diretiva visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela [Carta]. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º [desta].

[…]

(6) A Internet está a derrubar as tradicionais estruturas do mercado, proporcionando uma infraestrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações eletrónicas. Os serviços de comunicações eletrónicas publicamente disponíveis através da internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade.

(7) No caso das redes de comunicações públicas, é necessário estabelecer disposições legislativas, regulamentares e técnicas específicas para a proteção dos direitos e liberdades fundamentais das pessoas singulares e dos interesses legítimos das pessoas coletivas, em especial no que respeita à

capacidade crescente em termos de armazenamento e de processamento informático de dados relativos a assinantes e utilizadores.

[…]

(11) Tal como 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 (JO 1995, L 281, p. 31)], a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito [da União]. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, [assinada em Roma, em 4 de novembro de 1950], segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.»

4 O artigo 1.º da Diretiva 2002/58, sob a epígrafe «Âmbito e objetivos», dispõe:

«1. A presente diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na [União Europeia].

2. Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva [95/46]. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

3. A presente diretiva não é aplicável a atividades fora do âmbito do Tratado [FUE], tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal.»

5 Nos termos do artigo 2.º da Diretiva 2002/58, intitulado «Definições»:

«Salvo disposição em contrário, são aplicáveis as definições constantes da Diretiva [95/46] e da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro) [(JO 2002, L 108, p. 33)].

São também aplicáveis as seguintes definições:

a) "Utilizador" é qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

b) "Dados de tráfego" são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma;

c) "Dados de localização" quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público;

d) "Comunicação" é qualquer informação trocada ou enviada entre um número finito de partes, através de um serviço de comunicações eletrónicas publicamente disponível; não se incluem aqui as informações enviadas no âmbito de um serviço de difusão ao público em geral, através de uma rede de comunicações eletrónicas, exceto na medida em que a informação possa ser relacionada com o assinante ou utilizador identificável que recebe a informação;

[…]»

6 O artigo 3.º da Diretiva 2002/58, sob a epígrafe «Serviços abrangidos», prevê:

«A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na [União], nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação.»

7 Nos termos do artigo 5.º da Diretiva 2002/58, sob a epígrafe «Confidencialidade das comunicações»:

«1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.

[…]

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva [95/46], nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»

8 O artigo 6.º da Diretiva 2002/58, sob a epígrafe «Dados de tráfego», dispõe:

«1. Sem prejuízo do disposto nos n.os 2, 3 e 5 do presente artigo e no n.º 1 do artigo 15.º, os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

2. Podem ser tratados dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações. O referido tratamento é lícito apenas até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.

3. Para efeitos de comercialização dos serviços de comunicações eletrónicas ou para a prestação de serviços de valor acrescentado, o prestador de um serviço de comunicações eletrónicas acessível ao público pode tratar os dados referidos no n.º 1 na medida do necessário e pelo tempo necessário para a prestação desses serviços ou essa comercialização, se o assinante ou utilizador a quem os dados dizem respeito tiver dado o seu consentimento prévio. Deve ser dada a possibilidade aos utilizadores ou assinantes de retirarem a qualquer momento o seu consentimento para o tratamento dos dados de tráfego.

[…]

5. O tratamento de dados de tráfego, em conformidade com o disposto nos n.os 1 a 4, será limitado ao pessoal que trabalha para os fornecedores de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis encarregado da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas publicamente disponíveis, ou da prestação de um serviço de valor acrescentado, devendo ser limitado ao necessário para efeitos das referidas atividades.

[…]»

9 O artigo 9.º desta diretiva, intitulado «Dados de localização para além dos dados de tráfego», prevê, no seu n.º 1:

«Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. […]»

10 O artigo 15.º da Diretiva 2002/58, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», enuncia, no seu n.º 1:

«Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva

[95/46]. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito [da União, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia.»

Direito irlandês

11 Como resulta do pedido de decisão prejudicial, a Lei de 2011 foi adotada para transpor para a ordem jurídica irlandesa a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54).

12 O artigo 1.º da Lei de 2011 define o termo «dados» como visando «os dados de tráfego ou os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador», e o termo «infração grave» como visando uma infração passível de pena de prisão de duração igual ou superior a cinco anos ou uma das outras infrações enumeradas no anexo 1 desta lei.

13 O artigo 3.º, n.º 1, da referida lei impõe a todos os prestadores de serviços de comunicações eletrónicas que conservem os dados referidos no seu anexo 2, parte 1, durante um período de dois anos e os dados referidos no seu anexo 2, parte 2, durante um ano.

14 O anexo 2, parte 1, da mesma lei visa, entre outros, os dados relativos às comunicações telefónicas nas redes fixa e móvel que permitem identificar a fonte e o destino de uma comunicação, determinar a data e a hora do início e do fim de uma comunicação, determinar o tipo de comunicação em causa e identificar o tipo e a localização geográfica do material de comunicação utilizado. Em especial, o ponto 6 deste anexo 2, parte 1, prevê a conservação dos dados necessários para localizar um meio de comunicação eletrónica móvel, sendo estes dados, por um lado, o identificador da célula e, por outro, dados que permitam determinar a localização geográfica das células, referindo-se à sua identidade de localização (identificador da célula), durante o período em que os dados de comunicação são conservados.

15 O anexo 2, parte 2, da Lei de 2011 visa os dados relativos ao acesso à Internet, o correio eletrónico e as comunicações telefónicas através da Internet e abrange, nomeadamente, os números de identificadores e de telefone, os endereços IP, bem como a data e a hora do início e do fim de uma comunicação. O teor das comunicações não está abrangido por este tipo de dados.

16 Por força dos artigos 4.º e 5.º da Lei de 2011, os prestadores de serviços de comunicações eletrónicas devem tomar determinadas medidas para garantir que os dados sejam protegidos contra os acessos não autorizados.

17 O artigo 6.º desta lei, que prevê as condições em que pode ser apresentado um pedido de acesso, dispõe, no seu n.º 1:

«Um agente da Polícia Nacional cuja posição não seja inferior à de superintendente-chefe pode pedir a um prestador de serviços que lhe comunique os dados conservados por esse prestador de serviços em conformidade com o artigo 3.º, se esse funcionário considerar que os dados em questão são necessários para efeitos:

(a) de prevenção, deteção, investigação ou repressão de uma infração grave,

(b) de salvaguarda da segurança do Estado,

(c) de preservação da vida humana.»

18 O artigo 7.º da referida lei obriga os prestadores de serviços de comunicações eletrónicas a deferir os pedidos referidos no seu artigo 6.º

19 Entre os mecanismos de controlo da decisão do agente da Polícia Nacional mencionados no artigo 6.º da Lei de 2011 figuram o procedimento de reclamação previsto no artigo 10.º desta lei, e o procedimento perante o *designated judge* (juiz designado), na aceção do seu artigo 12.º, ao qual incumbe fiscalizar a aplicação das disposições da referida lei.

Litígio no processo principal e questões prejudiciais

20 Em março de 2015, G.D. foi condenado a uma pena de prisão perpétua pelo homicídio de uma pessoa que havia desaparecido em agosto de 2012 e cujo cadáver só foi descoberto em setembro de 2013. No recurso da sua condenação, o interessado acusou nomeadamente o órgão jurisdicional de primeira instância de ter erradamente admitido como meios de prova dados de tráfego e dados de localização relativos a chamadas telefónicas, com o fundamento de que a Lei de 2011, que regulava a conservação desses dados e com base na qual os investigadores da Polícia Nacional tinham tido acesso aos referidos dados, violava os direitos que lhe são conferidos pelo direito da União. Este recurso está atualmente pendente.

21 Para poder impugnar, no âmbito do processo penal, a admissibilidade das referidas provas, G.D. instaurou na High Court (Tribunal Superior, Irlanda) uma ação cível com vista a obter a declaração da invalidade de determinadas disposições da Lei de 2011. Por Decisão de 6 de dezembro de 2018, esse órgão jurisdicional julgou procedente a argumentação de G.D. e considerou que o artigo 6.º, n.º 1, alínea a), desta lei era incompatível com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta. A Irlanda recorreu desta decisão para a Supreme Court (Supremo Tribunal, Irlanda), o órgão jurisdicional de reenvio.

22 O processo penal pendente na Court of Appeal (Tribunal de Recurso, Irlanda) foi suspenso até ser proferida a decisão do órgão jurisdicional de reenvio no âmbito da ação cível no processo principal.

23 Perante o órgão jurisdicional de reenvio, a Irlanda sustentou que, para determinar se a ingerência no direito ao respeito pela vida privada consagrado no artigo 7.º da Carta, resultante da conservação dos dados de tráfego e dos dados de localização ao abrigo da Lei de 2011, é proporcionada, há que examinar os objetivos do regime implementado por esta lei na sua globalidade. Além disso, segundo este Estado-Membro, a referida lei estabeleceu um quadro detalhado de regulação do acesso aos dados conservados, nos termos do qual a unidade da Polícia Nacional encarregada da apreciação prévia dos pedidos de acesso goza de independência funcional em relação à Polícia Nacional no exercício da sua missão

e, por conseguinte, satisfaz o requisito de um controlo prévio dos pedidos de acesso efetuado por uma entidade administrativa independente. Este sistema de controlo é reforçado por um procedimento de reclamação e por uma fiscalização jurisdicional. Por último, o referido Estado-Membro alega que se se considerar, em última instância, que a Lei de 2011 é contrária ao direito da União, qualquer declaração que seja dela deduzida pelo órgão jurisdicional de reenvio deverá ter, do ponto de vista dos seus efeitos, eficácia meramente prospetiva.

24 Por seu turno, G.D. alegou que o regime de conservação generalizada e indiferenciada dos dados instituído pela Lei de 2011, bem como o regime de acesso a esses dados previsto por esta lei, são incompatíveis com o direito da União, conforme interpretado em especial pelo Tribunal de Justiça no n.º 120 do Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970).

25 O órgão jurisdicional de reenvio precisa, a título preliminar, que lhe compete apenas apreciar se a High Court (Tribunal Superior) decidiu corretamente que o artigo 6.º, n.º 1, alínea a), da Lei de 2011 é incompatível com o direito da União e que, em contrapartida, a questão da admissibilidade dos meios de prova invocados no âmbito do processo penal é da exclusiva competência da Court of Appeal (Tribunal de Recurso), chamada a decidir o recurso interposto da decisão de condenação.

26 Neste contexto, o órgão jurisdicional de reenvio interroga-se, antes de mais, sobre os requisitos do direito da União no que respeita à conservação dos dados para efeitos de luta contra a criminalidade grave. A este respeito, considera, em substância, que só uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização permite lutar, de modo efetivo, contra a criminalidade grave, o que uma conservação seletiva e uma conservação rápida (*quick freeze*) não permitem fazer. No que respeita à conservação seletiva, o órgão jurisdicional de reenvio interroga-se sobre a possibilidade de visar grupos ou zonas geográficas determinados para efeitos de luta contra a criminalidade grave, na medida em que certas infrações graves raramente implicam circunstâncias conhecidas das autoridades nacionais competentes que lhes permitam suspeitar da prática de uma infração antes de esta ser cometida. Além disso, uma conservação seletiva pode dar lugar a discriminações. Quanto à conservação rápida, o órgão jurisdicional de reenvio considera que esta só é útil em situações em que exista um suspeito identificável numa fase precoce do inquérito.

27 No que respeita, em seguida, ao acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas, o órgão jurisdicional de reenvio sublinha que a Polícia Nacional instituiu, internamente, um mecanismo de autocertificação dos pedidos de acesso dirigidos a esses prestadores. Assim, resulta dos elementos apresentados na High Court (Tribunal Superior) que o chefe da Polícia Nacional decidiu, a título de medida interna, que os pedidos de acesso apresentados ao abrigo da Lei de 2011 devem ser objeto de um tratamento centralizado por um único agente da Polícia Nacional, com a qualidade de superintendente-chefe, ou seja, o chefe do Departamento de Segurança e Informações. Se este último considerar que os dados em causa são necessários para efeitos, nomeadamente, de prevenção, deteção, investigação ou repressão de uma infração grave, pode apresentar um pedido de acesso aos prestadores de serviços de comunicações eletrónicas. Por outro lado, o chefe da Polícia Nacional instituiu, também

internamente, uma unidade independente denominada *Telecommunications Liaison Unit* (Unidade de Ligação das Telecomunicações, a seguir «TLU»), a fim de prestar apoio ao chefe do Departamento de Segurança e Informações no exercício das suas funções e de servir de ponto de contacto único com esses mesmos prestadores de serviços.

28 O órgão jurisdicional de reenvio acrescenta que, durante o período abrangido pelo inquérito penal instaurado contra G.D., todos os pedidos de acesso deviam ser aprovados, em primeiro lugar, por um superintendente ou por um inspetor que atuasse nessa qualidade, antes de serem enviados à TLU com vista ao seu tratamento, e que os investigadores eram aconselhados a incluir nos seus pedidos de acesso detalhes suficientes para que pudesse ser tomada uma decisão informada. Além disso, a TLU e o chefe do Departamento de Segurança e Informações eram obrigados a examinar a legalidade, a necessidade e a proporcionalidade dos pedidos de acesso, tendo em conta o facto de que esse chefe podia ser chamado a responder pela sua decisão perante um juiz designado pela High Court (Tribunal Superior). Por outro lado, a TLU estava sujeita ao controlo do Data Protection Commissioner (Comissário para a Proteção de Dados, Irlanda).

29 Por último, o órgão jurisdicional de reenvio interroga-se sobre o alcance e os efeitos no tempo de uma eventual declaração de não conformidade da Lei de 2011 com o direito da União. A este respeito, precisa que essa declaração só pode ter efeitos prospetivos, pelo facto de os dados utilizados como provas no processo penal conta G.D. terem sido objeto de conservação e de acesso no final de 2013, ou seja num período em que a Irlanda estava obrigada a aplicar as disposições da Lei de 2011 que transpôs a Diretiva 2006/24. Segundo a Irlanda, essa solução também é adequada na medida em que, caso contrário, a investigação e a repressão das infrações graves na Irlanda, bem como a situação das pessoas já julgadas e condenadas, poderiam ser seriamente afetadas.

30 Foi nestas circunstâncias que a Supreme Court (Supremo Tribunal, Irlanda) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Um regime geral ou universal de conservação de dados, ainda que sujeito a limitações estritas em matéria de conservação e acesso, é, em si mesmo, contrário ao disposto no artigo 15.º da Diretiva [2002/58], conforme interpretado à luz da [Carta]?

2) Ao apreciar a eventual incompatibilidade de uma medida nacional implementada nos termos da Diretiva [2006/24], que prevê um regime geral de conservação de dados (sujeito a controlos rigorosos necessários em matéria de conservação e/ou acesso) e, em especial, ao avaliar a proporcionalidade de tal regime, pode um órgão jurisdicional nacional ter em conta o facto de os dados poderem ser licitamente conservados por prestadores de serviços para os seus próprios fins comerciais, e poderem ter de ser conservados por razões de segurança nacional excluídas [do âmbito de aplicação] das disposições da Diretiva [2002/58]?

3) Ao apreciar a eventual compatibilidade de uma medida nacional de acesso a dados conservados com o direito da União e, em especial, com a [Carta], que critérios deve o órgão jurisdicional nacional aplicar para verificar se esse regime de acesso prevê o controlo prévio independente exigido pelo Tribunal de Justiça em conformidade com a sua jurisprudência? Neste contexto, pode um órgão jurisdicional nacional, no âmbito dessa apreciação, ter em conta a existência de um[a] [fiscalização jurisdicional] ou independente *ex post*?

4) Em qualquer caso, está um órgão jurisdicional nacional obrigado a declarar a incompatibilidade de uma medida nacional com o disposto no artigo 15.º da Diretiva [2002/58], se a medida nacional previr um regime geral de conservação de dados com o objetivo de [luta contra a criminalidade grave], e quando o órgão jurisdicional nacional tiver concluído, com base em todos os meios de prova disponíveis, que essa conservação é simultaneamente indispensável e estritamente necessária à concretização do objetivo de [luta contra a criminalidade grave]?

5) Se um órgão jurisdicional nacional se vir obrigado a concluir que uma medida nacional é incompatível com o disposto no artigo 15.º da Diretiva [2002/58], conforme interpretado à luz da [Carta], pode este limitar os efeitos no tempo dessa declaração, caso considere que não fazê-lo redundaria em «caos e prejuízo para o interesse geral» [em consonância com a abordagem seguida, por exemplo, no processo R (*National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, n.º 46]?

6) Pode um órgão jurisdicional nacional chamado a declarar a incompatibilidade da legislação nacional com o artigo 15.º da Diretiva [2002/58], e/ou a não aplicar essa legislação, e/ou a declarar que a aplicação dessa legislação violou os direitos de um particular, no contexto de um processo instaurado para promover um debate sobre a admissibilidade de meios de prova no âmbito de um processo penal ou noutras circunstâncias, ser autorizado a julgar improcedente essa pretensão no que respeita aos dados conservados em aplicação da disposição nacional adotada ao abrigo da obrigação prevista no artigo 288.º TFUE de transpor fielmente para o direito nacional as disposições de uma diretiva, ou a limitar os efeitos dessa declaração ao período subsequente ao da declaração da invalidade da Diretiva [2006/24] proferida pelo [Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238)]?»

Quanto às questões prejudiciais

Quanto à primeira, segunda e quarta questões

31 Com a primeira, segunda e quarta questões, que importa examinar em conjunto, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional que prevê uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização para efeitos de luta contra a criminalidade grave.

32 Importa recordar, a título preliminar, que é jurisprudência constante que, para interpretar uma disposição do direito da União, há que ter em conta não só os seus termos mas também o seu contexto e os objetivos prosseguidos pela regulamentação de que a mesma faz parte e, nomeadamente, a génese dessa regulamentação (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 105 e jurisprudência referida).

33 Resulta dos próprios termos do artigo 15.º, n.º 1, da Diretiva 2002/58 que as medidas legislativas que esta autoriza os Estados-Membros a adotar, nas condições nela

fixadas, apenas podem ter por objetivo «restringir o âmbito» dos direitos e obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58.

34 No que respeita ao sistema instituído por esta diretiva e no qual se insere o seu artigo 15.º, n.º 1, há que recordar que, nos termos do artigo 5.º, n.º 1, primeira e segunda frases, da referida diretiva, os Estados-Membros são obrigados a garantir, através da respetiva legislação nacional, a confidencialidade das comunicações realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis, bem como a confidencialidade dos respetivos dados de tráfego. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º da mesma diretiva.

35 A este respeito, o Tribunal de Justiça já declarou que o artigo 5.º, n.º 1, da Diretiva 2002/58 consagra o princípio da confidencialidade tanto das comunicações eletrónicas como dos respetivos dados de tráfego e implica, nomeadamente, que, em princípio, pessoas que não os utilizadores estejam proibidas de armazenar, sem o consentimento destes, essas comunicações e esses dados (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 107).

36 Esta disposição reflete o objetivo prosseguido pelo legislador da União quando da adoção da Diretiva 2002/58. Com efeito, resulta da exposição de motivos da proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas [COM(2000) 385 final], que está na origem da Diretiva 2002/58, que o legislador da União pretendeu «assegurar a continuação de um elevado nível de proteção dos dados pessoais e da privacidade no que diz respeito a todos os serviços de comunicações eletrónicas, independentemente da tecnologia utilizada». A referida diretiva tem assim por finalidade, como resulta, nomeadamente, dos seus considerandos 6 e 7, proteger os utilizadores dos serviços de comunicações eletrónicas contra os riscos para os seus dados pessoais e a sua vida privada resultantes das novas tecnologias, nomeadamente da capacidade crescente em termos de armazenamento e de processamento informático de dados. Em particular, como enuncia o considerando 2 da mesma diretiva, a intenção do legislador da União é de assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º da Carta (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 83, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 106).

37 Assim, ao adotar a Diretiva 2002/58, o legislador da União concretizou estes direitos, pelo que os utilizadores dos meios de comunicações eletrónicos têm o direito de esperar, em princípio, que, caso não tenham dado consentimento, as suas comunicações e respetivos dados permaneçam anónimos e não possam ser objeto de registo (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 109).

38 No que respeita ao tratamento e ao armazenamento pelos prestadores de serviços de comunicações eletrónicas dos dados de tráfego relativos a assinantes e utilizadores, o artigo 6.º da Diretiva 2002/58 prevê, no seu n.º 1, que esses dados devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação, e precisa, no seu n.º 2, que os dados

de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações só podem ser tratados até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado. No que se refere aos dados de localização para além dos dados de tráfego, o artigo 9.º, n.º 1, da referida diretiva estabelece que esses dados só podem ser tratados em determinadas condições e depois de serem tornados anónimos ou com o consentimento dos utilizadores ou assinantes.

39 Por conseguinte, a Diretiva 2002/58 não se limita a enquadrar o acesso a esses dados através de garantias destinadas a prevenir abusos, mas consagra também, em especial, o princípio da proibição do seu armazenamento por terceiros.

40 Na medida em que o artigo 15.º, n.º 1, da Diretiva 2002/58 permite aos Estados-Membros adotar medidas legislativas destinadas a «restringir o âmbito» dos direitos e obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º desta diretiva, como os que decorrem dos princípios da confidencialidade das comunicações e da proibição de armazenamento dos respetivos dados, recordados no n.º 35 do presente acórdão, esta disposição enuncia uma exceção à regra geral prevista nomeadamente nestes artigos 5.º, 6.º e 9.º e deve, assim, em conformidade com jurisprudência constante, ser objeto de interpretação estrita. Esta disposição não pode, portanto, justificar que a derrogação da obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados e, em especial, a proibição de armazenar esses dados, prevista no artigo 5.º dessa diretiva, se converta em regra, sob pena de esvaziar em grande medida esta última disposição do seu alcance (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 89, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 111).

41 Quanto aos objetivos suscetíveis de justificar uma restrição dos direitos e das obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58, o Tribunal de Justiça já declarou que a enumeração dos objetivos que figuram no artigo 15.º, n.º 1, primeira frase, desta diretiva tem caráter taxativo, de modo que uma medida legislativa adotada ao abrigo desta disposição tem que responder efetiva e estritamente a um desses objetivos (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 112 e jurisprudência referida).

42 Além disso, resulta do artigo 15.º, n.º 1, terceira frase, da Diretiva 2002/58 que as medidas tomadas pelos Estados-Membros ao abrigo desta disposição devem respeitar os princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e assegurar o respeito dos direitos fundamentais garantidos pela Carta. A este respeito, o Tribunal de Justiça já declarou que a obrigação imposta por um Estado-Membro aos prestadores de serviços de comunicações eletrónicas, através de uma regulamentação nacional, de conservarem os dados de tráfego para, se for caso disso, os disponibilizarem às autoridades nacionais competentes coloca questões não apenas quanto ao respeito dos artigos 7.º e 8.º da Carta, relativos, respetivamente, à proteção da vida privada e à proteção dos dados pessoais, mas igualmente do artigo 11.º da Carta, relativo à liberdade de expressão (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C 512/18 e C 520/18, EU:C:2020:791, n.º 113 e jurisprudência referida).

43 Assim, a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 deve ter em conta a importância tanto do direito ao respeito da vida privada, garantido pelo artigo 7.º da Carta, como do direito à proteção dos dados pessoais, garantido pelo artigo 8.º da mesma, conforme resulta da jurisprudência do Tribunal de Justiça, assim como do direito à liberdade de expressão, direito fundamental, garantido pelo artigo 11.º da Carta, que constitui um dos fundamentos essenciais de uma sociedade democrática e pluralista, fazendo parte dos valores nos quais, em conformidade com o artigo 2.º TUE, se baseia a União (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C 512/18 e C-520/18, EU:C:2020:791, n.º 114 e jurisprudência referida).

44 Importa precisar, a este respeito, que a conservação de dados de tráfego e de dados de localização constitui, em si mesma, por um lado, uma derrogação da proibição, prevista no artigo 5.º, n.º 1, da Diretiva 2002/58, imposta a qualquer pessoa distinta dos utilizadores de armazenar estes dados e, por outro, uma ingerência nos direitos fundamentais do respeito pela vida privada e da proteção dos dados pessoais, consagrados nos artigos 7.º e 8.º da Carta, não sendo importante que as informações relativas à vida privada em questão sejam ou não sensíveis, ou que os interessados tenham ou não sofrido inconvenientes em razão dessa ingerência, ou ainda que os dados conservados sejam ou não utilizados posteriormente (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 115, 116 e jurisprudência referida).

45 Esta conclusão revela-se ainda mais justificada quando os dados de tráfego e os dados de localização são suscetíveis de revelar informações sobre um número significativo de aspetos da vida privada das pessoas em causa, incluindo informações sensíveis, tais como a orientação sexual, as opiniões políticas, as convicções religiosas, filosóficas, sociais ou outras, bem como o estado de saúde, uma vez que tais dados beneficiam, além disso, de uma proteção especial no direito da União. Considerados no seu todo, estes dados podem permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de modo permanente ou temporário, as deslocações diárias ou outras, as atividades exercidas, as relações sociais dessas pessoas e os meios sociais que frequentam. Em especial, estes dados fornecem os meios para determinar o perfil das pessoas em causa, informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 117 e jurisprudência referida).

46 Por conseguinte, por um lado, a conservação de dados de tráfego e de dados de localização para fins policiais é suscetível de violar o direito ao respeito das comunicações, consagrado no artigo 7.º da Carta, e de produzir efeitos dissuasivos sobre o exercício, pelos utilizadores dos meios de comunicações eletrónicos, da sua liberdade de expressão, garantida no artigo 11.º da referida Carta, efeitos estes que são tanto mais graves quanto maiores sejam o número e a variedade dos dados conservados. Por outro lado, tendo em conta a quantidade significativa de dados de tráfego e de dados de localização que podem ser conservados de modo contínuo através de uma medida de conservação generalizada e indiferenciada, assim como o caráter sensível das informações que esses dados podem fornecer, a mera conservação dos referidos dados pelos prestadores de serviços de comunicações eletrónicas comporta riscos de abuso e de acesso ilícito (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 118, 119 e jurisprudência referida).

47 A este respeito, há que sublinhar que a conservação destes dados e o acesso aos mesmos constituem, como resulta da jurisprudência recordada no n.º 44 do presente acórdão, ingerências distintas nos direitos fundamentais garantidos nos artigos 7.º e 11.º da Carta, que necessitam de uma justificação distinta, nos termos do artigo 52.º, n.º 1, da mesma. Daqui decorre que uma legislação nacional que assegura o pleno respeito das condições que resultam da jurisprudência que interpretou a Diretiva 2002/58 em matéria de acesso aos dados conservados não pode, por natureza, ser suscetível de restringir nem sequer de corrigir a ingerência grave, que resultaria da conservação generalizada desses dados prevista por esta legislação nacional, nos direitos garantidos nos artigos 6.º e 5.º desta diretiva e pelos direitos fundamentais de que esses artigos constituem a concretização.

48 Não obstante, na medida em que permite aos Estados-Membros restringir os direitos e obrigações referidos nos n.ºs 34 a 37 do presente acórdão, o artigo 15.º, n.º 1, da Diretiva 2002/58 reflete a circunstância de os direitos consagrados nos artigos 7.º, 8.º e 11.º da Carta não serem prerrogativas absolutas, mas deverem ser tomados em consideração relativamente à sua função na sociedade. Com efeito, conforme resulta do seu artigo 52.º, n.º 1, a Carta admite restrições ao exercício desses direitos, desde que essas restrições estejam previstas por lei, respeitem o conteúdo essencial desses direitos e, na observância do princípio da proporcionalidade, sejam necessárias e correspondam efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros. Assim, a interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58 à luz da Carta exige que se tenha em conta igualmente a importância dos direitos consagrados nos artigos 3.º, 4.º, 6.º e 7.º da Carta e a importância dos objetivos de proteção da segurança nacional e de luta contra a criminalidade grave, contribuindo para a proteção dos direitos e liberdades de terceiros (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.ºs 120 a 122 e jurisprudência referida).

49 Assim, no que no que diz respeito, em particular, à luta efetiva contra as infrações penais de que são vítimas, nomeadamente, menores e outras pessoas vulneráveis, importa ter em conta o facto de que podem resultar do artigo 7.º da Carta obrigações positivas que incumbem aos poderes públicos, tendo em vista a adoção de medidas jurídicas destinadas a proteger a vida privada e familiar. Tais obrigações são igualmente suscetíveis de decorrer do referido artigo 7.º no que diz respeito à proteção do domicílio e das comunicações, bem como dos artigos 3.º e 4.º, relativos à proteção da integridade física e psíquica das pessoas e à proibição da tortura e dos tratos desumanos e degradantes (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.º 126 e jurisprudência referida).

50 Face a estas diferentes obrigações positivas, há, portanto, que proceder a uma conciliação dos diferentes interesses legítimos e direitos em causa. Com efeito, o Tribunal Europeu dos Direitos do Homem declarou que as obrigações positivas decorrentes dos artigos 3.º e 8.º da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, cujas garantias correspondentes figuram nos artigos 4.º e 7.º da Carta, implicam, nomeadamente, a adoção de disposições materiais e processuais, assim como de medidas de ordem prática que permitam combater eficazmente os crimes contra as pessoas através de uma investigação e de processos efetivos, sendo esta obrigação ainda mais importante

quando o bem-estar físico e moral de uma criança é ameaçado. Não obstante, as medidas que cabe às autoridades competentes adotar devem respeitar plenamente as vias de recurso e outras garantias suscetíveis de limitar o âmbito dos poderes de investigações penais e as outras liberdades e direitos. Em particular, segundo esse tribunal, deve instituir-se um quadro jurídico que permita conciliar os diferentes interesses legítimos e direitos a proteger (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 127, 128 e jurisprudência referida).

51 Neste quadro, decorre dos próprios termos do artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58 que os Estados-Membros podem adotar uma medida derrogatória do princípio da confidencialidade evocado no n.º 35 do presente acórdão quando tal medida seja «necessária, adequada e proporcionada numa sociedade democrática», indicando o considerando 11 desta diretiva, a este respeito, que uma medida desta natureza deve ser «rigorosamente» proporcionada ao objetivo a alcançar (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 129).

52 A este respeito, importa recordar que a proteção do direito fundamental ao respeito da vida privada impõe, em conformidade com a jurisprudência constante do Tribunal de Justiça, que as derrogações à proteção dos dados pessoais e as respetivas restrições ocorram na estrita medida do necessário. Além disso, um objetivo de interesse geral não pode ser prosseguido sem se ter em conta o facto de que deve ser conciliado com os direitos fundamentais abrangidos pela medida, mediante uma ponderação equilibrada entre o objetivo e os interesses e direitos em causa (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 130 e jurisprudência referida).

53 Mais particularmente, decorre da jurisprudência do Tribunal de Justiça que a possibilidade de os Estados-Membros justificarem uma restrição aos direitos e às obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 deve ser apreciada através da medição da gravidade da ingerência que tal restrição implica e da verificação de que a importância do objetivo de interesse geral prosseguido por esta restrição está relacionada com essa gravidade (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 131 e jurisprudência referida).

54 Para cumprir a exigência de proporcionalidade, uma legislação nacional deve prever normas claras e precisas que regulem o âmbito e a aplicação da medida em causa e impor requisitos mínimos, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Essa legislação deve ser vinculativa no direito interno e, em particular, indicar em que circunstâncias e em que condições uma medida que prevê o tratamento de tais dados pode ser adotada, garantindo assim que a ingerência seja limitada ao estritamente necessário. A necessidade de dispor de tais garantias é ainda maior quando os dados pessoais são sujeitos a um processamento informático, nomeadamente quando existe um risco significativo de acesso ilícito a tais dados. Estas considerações são particularmente válidas quando está em jogo a proteção desta categoria específica de dados pessoais, que são os dados sensíveis (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 132 e jurisprudência referida).

55 Assim, uma legislação nacional que preveja uma conservação dos dados pessoais deve responder sempre a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido. Em particular, no que respeita à luta

contra a criminalidade grave, os dados cuja conservação está prevista devem ser suscetíveis de contribuir para a prevenção, a deteção ou a repressão de infrações graves (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 59, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 133).

56 Relativamente aos objetivos de interesse geral suscetíveis de justificar uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, resulta da jurisprudência do Tribunal de Justiça, em especial do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), que, em conformidade com o princípio da proporcionalidade, existe uma hierarquia entre estes objetivos em função da sua importância respetiva e que a importância do objetivo prosseguido por essa medida deve estar relacionada com a gravidade da ingerência daí resultante.

57 A este respeito, o Tribunal de Justiça declarou que a importância do objetivo de salvaguarda da segurança nacional, lido à luz do artigo 4.º, n.º 2, TUE, ultrapassa a dos outros objetivos referidos no artigo 15.º, n.º 1, da Diretiva 2002/58, nomeadamente os objetivos de luta contra a criminalidade em geral, incluindo grave, e de salvaguarda da segurança pública. Sem prejuízo do respeito dos outros requisitos previstos no artigo 52.º, n.º 1, da Carta, o objetivo de salvaguarda da segurança nacional é, por conseguinte, suscetível de justificar medidas que incluem ingerências nos direitos fundamentais mais graves do que aquelas que esses outros objetivos poderiam justificar (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.ºs 135 e 136).

58 É por este motivo que o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que permitam, para efeitos de salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas que procedam a uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, quando o Estado-Membro em causa enfrente uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, quando a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva quer por um órgão jurisdicional quer por uma entidade administrativa efetiva independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma dessas situações e o respeito dos requisitos e das garantias que devem estar previstos, e quando a referida imposição apenas possa ser aplicada por um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 168).

59 No que diz respeito ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, o Tribunal de Justiça salientou que, em conformidade com o princípio da proporcionalidade, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis de justificar ingerências graves nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, tais como as que implicam a conservação de dados de tráfego e de dados de localização. Por conseguinte, só as ingerências sem caráter grave nos

referidos direitos fundamentais podem ser justificadas pelo objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral regulamentação em causa no processo principal, de prevenção, de investigação, de deteção e perseguição de infrações penais em geral (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.º 140 e jurisprudência referida).

60 Na audiência, a Comissão Europeia sustentou que a criminalidade particularmente grave pode ser equiparada a uma ameaça para a segurança nacional.

61 Ora, o Tribunal de Justiça já declarou que o objetivo de preservação da segurança nacional corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade, através da prevenção e a repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal, como, nomeadamente, as atividades terroristas (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 135).

62 Além disso, há que salientar que, diversamente da criminalidade, mesmo particularmente grave, uma ameaça para a segurança nacional deve ser real e atual ou, pelo menos, previsível, o que pressupõe a ocorrência de circunstâncias suficientemente concretas, para poder justificar uma medida de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, durante um período limitado. Essa ameaça distingue-se, portanto, pela sua natureza, a sua gravidade e o caráter específico das circunstâncias que a constituem, do risco geral e permanente de ocorrência de tensões ou de perturbações, ainda que graves, à segurança pública ou do risco de infrações penais graves (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.ºs 136 e 137).

63 Assim, a criminalidade, ainda que particularmente grave, não pode ser equiparada a uma ameaça para a segurança nacional. Com efeito, como salientou o advogado-geral nos n.ºs 49 e 50 das suas conclusões, essa equiparação seria suscetível de introduzir uma categoria intermédia entre a segurança nacional e a segurança pública, para aplicar à segunda as exigências inerentes à primeira.

64 Daqui resulta igualmente que a circunstância, mencionada na segunda questão prejudicial, de os dados de tráfego e de os dados de localização terem sido legalmente objeto de uma conservação para efeitos de salvaguarda da segurança nacional não tem incidência na licitude da sua conservação para efeitos da luta contra a criminalidade grave.

65 No que respeita ao objetivo de luta contra a criminalidade grave, o Tribunal de Justiça declarou que uma legislação nacional que prevê, para este efeito, a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática. Com efeito, tendo em conta o caráter sensível das informações que os dados de tráfego e os dados de localização podem fornecer, a sua confidencialidade é essencial para o direito ao respeito da vida privada. Assim, e atendendo, por um lado, aos efeitos dissuasivos no exercício dos direitos fundamentais consagrados nos artigos 7.º e 11.º da Carta, referidos no n.º 46 do presente acórdão, que a conservação desses dados pode

produzir e, por outro, à gravidade da ingerência que tal conservação implica, é necessário, numa sociedade democrática, que esta seja a exceção e não a regra, como prevê o sistema instituído pela Diretiva 2002/58, e que esses dados não possam ser objeto de uma conservação sistemática e contínua. Esta conclusão impõe-se mesmo em relação aos objetivos de luta contra a criminalidade grave e de prevenção das ameaças graves contra a segurança pública, bem como à importância que lhes deve ser reconhecida (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.os 141, 142 e jurisprudência referida).

66 Além disso, o Tribunal de Justiça sublinhou que uma legislação nacional que prevê a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização abrange as comunicações eletrónicas de quase toda a população sem que seja estabelecida nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido. Tal legislação afeta globalmente todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que essas pessoas se encontrem, mesmo indiretamente, numa situação suscetível de justificar um procedimento penal. Por conseguinte, aplica-se inclusivamente a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com este objetivo de luta contra os atos de criminalidade grave e, em particular, sem que se estabeleça uma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública. Em particular, como já declarou o Tribunal de Justiça, tal legislação não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de algum modo numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade grave (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.os 143, 144 e jurisprudência referida).

67 Em contrapartida, no n.º 168 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791), o Tribunal de Justiça precisou que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 8.º, 7.º e 11.º e do artigo 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

— uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

— uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

— uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

— uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida (*quick freeze*) dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem;

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

68 No presente pedido prejudicial, que deu entrada no Tribunal de Justiça antes da prolação dos Acórdãos de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), e de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152), o órgão jurisdicional de reenvio considerou, contudo, que só a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização de dados de tráfego permitia lutar, de maneira efetiva, contra a criminalidade grave. Na audiência de 13 de setembro de 2021, foi defendido, nomeadamente pela Irlanda e pelo Governo francês, que essa conclusão não era infirmada pelo facto de os Estados-Membros poderem recorrer às medidas referidas no número anterior.

69 A este respeito, importa salientar, em primeiro lugar, que a eficácia de processos penais depende geralmente não de um único instrumento de investigação, mas de todos os instrumentos de investigação de que dispõem as autoridades nacionais competentes para esses efeitos.

70 Em segundo lugar, há que sublinhar que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e do artigo 52.º, n.º 1, da Carta, conforme interpretado pela jurisprudência recordada no n.º 67 do presente acórdão, permite que os Estados-Membros adotem, para efeitos da luta contra a criminalidade grave e a prevenção de ameaças graves contra a segurança pública, não só medidas que instituam uma conservação seletiva e uma conservação rápida, mas também medidas que prevejam uma conservação generalizada e indiferenciada, por um lado, de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos e, por outro, de endereços IP atribuídos à fonte de uma ligação.

71 A este respeito, é pacífico que a conservação dos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicas é suscetível de contribuir para a luta contra a criminalidade grave, desde que esses dados permitam identificar as pessoas que utilizaram esses meios no contexto da preparação ou da prática de um ato de criminalidade grave.

72 Ora, como resulta da jurisprudência resumida no n.º 67 do presente acórdão, a Diretiva 2002/58 não se opõe, para efeitos da luta contra a criminalidade em geral, à conservação generalizada dos dados relativos à identidade civil. Nestas condições, há que precisar que nem esta diretiva nem nenhum outro ato do direito da União se opõem a uma legislação nacional que tenha por objeto a luta contra a criminalidade grave, nos termos da qual a aquisição de um meio de comunicação eletrónica, como um cartão SIM pré-pago, esteja sujeita à verificação de documentos oficiais que comprovem a identidade do comprador e ao registo, pelo vendedor, das informações daí resultantes, sendo o vendedor obrigado, se for caso disso, a dar acesso a essas informações às autoridades nacionais competentes.

73 Além disso, há que recordar que a conservação generalizada dos endereços IP atribuídos à fonte da ligação constitui uma ingerência grave nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, uma vez que esses endereços IP podem permitir tirar conclusões precisas sobre a vida privada do utilizador do meio de comunicação eletrónica em causa e ter efeitos dissuasivos no exercício da liberdade de expressão garantida no artigo 11.º da mesma. Todavia, no que respeita a essa conservação, o Tribunal de Justiça declarou que, para efeitos da necessária conciliação dos direitos e dos interesses em causa exigida pela jurisprudência referida nos n.ºs 50 a 53 do presente acórdão, há que ter em conta o facto de, no caso de uma infração cometida em linha e, em especial, no caso da aquisição, da difusão, da transmissão ou da colocação à disposição em linha de pornografia infantil, na aceção do artigo 2.º, alínea c), da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO 2011, L 335, p. 1), o endereço IP poder constituir o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática dessa infração (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, EU:C:2020:791, n.ºs 153 e 154).

74 Por conseguinte, o Tribunal de Justiça declarou que essa conservação generalizada e indiferenciada apenas dos endereços IP atribuídos à fonte de uma ligação não se afigura, em princípio, contrária ao artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º da Carta, desde que essa possibilidade esteja sujeita ao estrito respeito das condições materiais e processuais que devem reger a utilização desses dados referidos nos n.ºs 155 e 156 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

75 Em terceiro lugar, no que respeita às medidas legislativas que preveem uma conservação seletiva e uma conservação rápida dos dados de tráfego e dos dados de localização, as indicações que figuram no pedido de decisão prejudicial revelam um entendimento mais estreito do alcance destas medidas do que o acolhido pela jurisprudência recordada no n.º 67 do presente acórdão. Com efeito, embora, em conformidade com o que foi recordado no n.º 40 do presente acórdão, estas medidas de conservação devam apresentar um caráter derrogatório no sistema instituído pela Diretiva 2002/58, esta, lida à luz dos direitos fundamentais consagrados nos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não subordina a possibilidade de impor uma conservação seletiva à condição de serem conhecidos, antecipadamente, os locais suscetíveis de serem a cena de um ato de criminalidade grave nem as pessoas suspeitas de estar implicadas nesse ato. Do mesmo modo, a referida diretiva não exige que a imposição de uma conservação rápida seja limitada a suspeitos identificados previamente a essa imposição.

76 No que respeita, em primeiro lugar, à conservação seletiva, o Tribunal de Justiça declarou que o artigo 15.º, n.º 1, da Diretiva 2002/58 não se opõe a uma legislação nacional baseada em elementos objetivos, que permitam visar, por um lado, as pessoas cujos dados de tráfego e dados de localização são suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública ou ainda um risco para a segurança nacional (Acórdãos de 21

de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 111, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 148).

77 O Tribunal de Justiça precisou, a este respeito que, embora esses elementos objetivos possam variar em função de medidas adotadas para efeitos da prevenção, da investigação, da deteção e da repressão da criminalidade grave, as pessoas assim visadas podem ser, nomeadamente, aquelas que foram previamente identificadas, no âmbito dos processos nacionais aplicáveis e com base em elementos objetivos, e não discriminatórios, como uma ameaça para a segurança pública ou para a segurança nacional do Estado-Membro em causa (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 110, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 149).

78 Os Estados-Membros têm assim, nomeadamente, a faculdade de adotar medidas de conservação contra pessoas que, a título dessa identificação, sejam objeto de um inquérito ou de outras medidas de vigilância atuais ou de inscrição no registo criminal nacional que mencione uma condenação anterior por atos de criminalidade grave que possam implicar um risco elevado de reincidência. Ora, quando essa identificação se baseia em elementos objetivos e não discriminatórios, definidos pelo direito nacional, a conservação seletiva dirigida a pessoas assim identificadas é justificada.

79 Por outro lado, uma medida de conservação seletiva dos dados de tráfego e dos dados de localização pode, segundo a escolha do legislador nacional e no estrito respeito do princípio da proporcionalidade, assentar igualmente num critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos e não discriminatórios, que existe, numa ou em várias zonas geográficas, uma situação caracterizada por um risco elevado de preparação ou de prática de atos de criminalidade grave. Essas zonas podem ser, nomeadamente, locais caracterizados por um elevado número de atos de criminalidade grave, locais particularmente expostos à prática de atos de criminalidade grave, tais como locais ou infraestruturas frequentados regularmente por um número muito grande de pessoas, ou ainda locais estratégicos, como aeroportos, estações ou zonas de portagens (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 150 e jurisprudência referida).

80 Importa sublinhar que, segundo esta jurisprudência, as autoridades nacionais competentes podem adotar, relativamente às zonas referidas no número anterior, uma medida de conservação seletiva baseada num critério geográfico, como, nomeadamente, a taxa média de criminalidade numa zona geográfica, sem disporem necessariamente de indícios concretos relativos à preparação ou à prática, nas zonas em causa, de atos de criminalidade grave. Na medida em que uma conservação seletiva baseada nesse critério é suscetível de afetar, em função das infrações penais graves visadas e da situação específica dos respetivos Estados-Membros, simultaneamente locais caracterizados por um elevado número de atos de criminalidade grave e locais particularmente expostos à prática de tais atos, também não é, em princípio, suscetível de dar lugar a discriminações, uma vez que o critério relativo à taxa média de criminalidade grave não apresenta, por si só, nenhuma ligação com elementos potencialmente discriminatórios.

81 Além disso, e sobretudo, uma medida de conservação seletiva dirigida a locais ou infraestruturas regularmente frequentados por um número muito elevado de pessoas ou a locais estratégicos, como aeroportos, estações, portos marítimos ou

zonas de portagens, permite às autoridades competentes recolher dados de tráfego e, nomeadamente, dados de localização de todas as pessoas que utilizam, num determinado momento, um meio de comunicação eletrónica num desses locais. Assim, essa medida de conservação seletiva é suscetível de permitir às referidas autoridades obter, através do acesso aos dados assim conservados, informações sobre a presença dessas pessoas nos locais ou nas zonas geográficas visados por essa medida, bem como sobre as suas deslocações entre ou no interior destes e daí retirar, para efeitos da luta contra a criminalidade grave, conclusões sobre a sua presença e a sua atividade nesses locais ou zonas geográficas num dado momento durante o período de conservação.

82 Importa ainda salientar que as zonas geográficas visadas por essa conservação seletiva podem e, se for caso disso, devem ser alteradas em função da evolução das condições que justificaram a sua seleção, permitindo assim, nomeadamente, reagir às evoluções da luta contra a criminalidade grave. Com efeito, o Tribunal de Justiça já declarou que a duração das medidas de conservação seletiva descritas nos n.os 76 a 81 do presente acórdão não pode ultrapassar a estritamente necessária à luz do objetivo prosseguido e das circunstâncias que as justificam, sem prejuízo de uma eventual renovação devido ao facto de continuar a ser necessário proceder a essa conservação (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 151).

83 No que respeita à possibilidade de prever critérios distintivos diferentes de um critério pessoal ou geográfico para aplicar uma conservação seletiva dos dados de tráfego e dos dados de localização, não se pode excluir que outros critérios, objetivos e não discriminatórios, possam entrar em linha de conta para garantir que o âmbito de uma conservação seletiva se limite ao estritamente necessário e estabelecer uma ligação, pelo menos indireta, entre os atos de criminalidade grave e as pessoas cujos dados são conservados. Não obstante, uma vez que o artigo 15.º, n.º 1, da Diretiva 2002/58 visa medidas legislativas dos Estados-Membros, é a estes últimos e não ao Tribunal de Justiça que incumbe identificar esses critérios, entendendo-se que não pode ser reinstituída por este meio uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

84 Em todo o caso, como salientou o advogado-geral M. Campos Sánchez-Bordona no n.º 50 das suas Conclusões nos processos apensos SpaceNet e Telekom Deutschland (C-793/19 e C-794/19, EU:C:2021:939), a eventual existência de dificuldades para definir precisamente as hipóteses e as condições em que pode ser efetuada uma conservação seletiva não pode justificar que os Estados-Membros, fazendo da exceção uma regra, prevejam uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

85 Em segundo lugar, no que diz respeito à conservação rápida dos dados de tráfego e dos dados de localização tratados e armazenados pelos prestadores de serviços de comunicações eletrónicas com base nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58, ou nas medidas legislativas adotadas ao abrigo do artigo 15.º, n.º 1, desta diretiva, importa recordar que esses dados devem ser, em princípio, consoante o caso, apagados ou tornados anónimos no termo dos prazos legais em que devem ser realizados, em conformidade com as disposições nacionais que transpõem essa diretiva, o seu tratamento e a sua armazenagem. No entanto, o Tribunal de Justiça declarou que, durante esse tratamento e essa armazenagem, podem ocorrer

situações em que é necessário conservar os referidos dados para além desses prazos para efeitos do esclarecimento de infrações penais graves ou de ofensas à segurança nacional, tanto na situação em que essas infrações ou essas ofensas já foram detetadas como na situação em que, após uma apreciação objetiva de todas as circunstâncias pertinentes, se pode razoavelmente suspeitar da sua existência (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 160 e 161).

86 Nessa situação, os Estados-Membros podem, tendo em conta a necessária conciliação dos direitos e interesses legítimos em causa referida nos n.os 50 a 53 do presente acórdão, prever, numa legislação adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, a possibilidade, através de uma decisão da autoridade competente sujeita a uma fiscalização jurisdicional efetiva, de impor aos prestadores de serviços de comunicações eletrónicas o dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que dispõem.

87 Na medida em que a finalidade de tal conservação rápida deixe de corresponder às finalidades para as quais os dados foram inicialmente recolhidos e conservados e na medida em que qualquer tratamento de dados deve, nos termos do artigo 8.º, n.º 2, da Carta, responder a determinados objetivos, os Estados-Membros devem precisar, na sua legislação, a finalidade que justifica a conservação rápida de dados. Tendo em conta o caráter grave da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que tal conservação pode comportar, só a luta contra a criminalidade grave e, *a fortiori*, a salvaguarda da segurança nacional são suscetíveis de justificar essa ingerência, desde que essa medida e o acesso aos dados assim conservados respeitem os limites do estritamente necessário, conforme enunciados nos n.os 164 a 167 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

88 O Tribunal de Justiça precisou que uma medida de conservação desta natureza não deve ser limitada aos dados das pessoas identificadas previamente como apresentando uma ameaça para a segurança pública ou para a segurança nacional do Estado-Membro em causa ou das pessoas concretamente suspeitas de terem praticado um ato de criminalidade grave ou uma ofensa à segurança nacional. Com efeito, segundo o Tribunal de Justiça, embora deva respeitar o quadro instituído pelo artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, e tendo em conta as considerações que figuram no n.º 55 do presente acórdão, tal medida pode, se for essa a escolha do legislador e respeitando os limites do estritamente necessário, ser alargada aos dados de tráfego e aos dados de localização relativos a pessoas diferentes das que são suspeitas de ter planeado ou cometido uma infração grave ou uma ofensa à segurança nacional, desde que tais dados possam, com base em elementos objetivos e não discriminatórios, contribuir para o esclarecimento dessa infração ou dessa ofensa à segurança nacional, tais como os dados da vítima desta e do seu meio social ou profissional (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 165).

89 Assim, uma medida legislativa pode autorizar que se imponha aos prestadores de serviços de comunicações eletrónicas a conservação rápida dos dados de tráfego e dos dados de localização, nomeadamente, das pessoas com as quais, antes da ocorrência de uma ameaça grave para a segurança pública ou da prática de um ato de criminalidade grave, uma vítima tenha estado em contacto utilizando os seus meios de comunicações eletrónicas.

90 Tal conservação rápida pode, segundo a jurisprudência do Tribunal de Justiça recordada no n.º 88 do presente acórdão e nas mesmas condições visadas nesse número, igualmente ser alargada a zonas geográficas determinadas, como os locais da prática e da preparação da infração ou da ofensa à segurança nacional em causa. Importa precisar que podem ainda ser objeto dessa medida os dados de tráfego e os dados de localização relativos ao local onde uma pessoa, potencialmente vítima de um ato de criminalidade grave, desapareceu, desde que essa medida e o acesso aos dados assim conservados respeitem os limites do estritamente necessário para efeitos da luta contra a criminalidade grave ou a salvaguarda da segurança nacional, conforme enunciados nos n.os 164 a 167 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

91 Por outro lado, importa precisar que o artigo 15.º, n.º 1, da Diretiva 2002/58 não se opõe a que as autoridades nacionais competentes ordenem uma medida de conservação rápida desde a primeira fase do inquérito sobre uma ameaça grave para a segurança pública ou sobre um eventual ato de criminalidade grave, a saber, a partir do momento em que, segundo as disposições pertinentes do direito nacional, essas autoridades podem dar início a esse inquérito.

92 No que respeita à variedade das medidas de conservação dos dados de tráfego e dos dados de localização referidos no n.º 67 do presente acórdão, importa precisar que estas diferentes medidas podem, consoante a escolha do legislador nacional e respeitando os limites do estritamente necessário, ser aplicadas conjuntamente. Nestas condições, o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, conforme interpretado pela jurisprudência decorrente do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), não se opõe a uma combinação destas medidas.

93 Em quarto e último lugar, importa sublinhar que a proporcionalidade das medidas adotadas ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 exige, segundo a jurisprudência constante do Tribunal de Justiça, como recapitulada no Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), o respeito não apenas dos requisitos de adequação e de necessidade, como também do requisito relativo ao caráter proporcional destas medidas relativamente ao objetivo prosseguido.

94 Neste contexto, há que recordar que, no n.º 51 do seu Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238), o Tribunal de Justiça declarou que, embora a luta contra a criminalidade grave tenha uma importância primordial para garantir a segurança pública e embora a sua eficácia possa depender em larga medida da utilização das técnicas modernas de investigação, esse objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, como a que foi instituída pela Diretiva 2006/24, seja considerada necessária.

95 No mesmo sentido, o Tribunal de Justiça precisou, no n.º 145 do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), que mesmo as obrigações positivas dos Estados-Membros que

possam decorrer, consoante o caso, dos artigos 3.º, 4.º e 7.º da Carta e relativas, conforme referido no n.º 49 do presente acórdão, à aplicação de regras que permitem uma luta efetiva contra as infrações penais não podem justificar ingerências tão graves como as que comporta uma legislação nacional que prevê uma conservação de dados de tráfego e de dados de localização nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta de quase toda a população, sem que os dados das pessoas em causa sejam suscetíveis de revelar uma ligação, no mínimo indireta, com o objetivo prosseguido.

96 Na audiência, o Governo dinamarquês sustentou que as autoridades nacionais competentes deveriam poder aceder, para efeitos da luta contra a criminalidade grave, aos dados de tráfego e aos dados de localização que foram conservados de maneira generalizada e indiferenciada, em conformidade com a jurisprudência decorrente do Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 135 a 139), para dar resposta a uma ameaça grave para a segurança nacional que se revele real e atual ou previsível.

97 Importa, desde logo, salientar que o facto de autorizar o acesso, para efeitos da luta contra a criminalidade grave, a dados de tráfego e a dados de localização que foram conservados de maneira generalizada e indiferenciada faz depender esse acesso de circunstâncias alheias a esse objetivo, em função da existência ou não, no Estado-Membro em causa, de uma ameaça grave para a segurança nacional conforme referida no número anterior, quando, à luz apenas do objetivo de luta contra a criminalidade grave que deve justificar a conservação desses dados e o acesso aos mesmos, nada justifica uma diferença de tratamento, em particular entre os Estados-Membros.

98 Como o Tribunal de Justiça já declarou, o acesso a dados de tráfego e a dados de localização conservados pelos prestadores em aplicação de uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, que deve ser efetuado no pleno respeito das condições resultantes da jurisprudência que interpretou a Diretiva 2002/58, apenas pode, em princípio, ser justificado pelo objetivo de interesse geral pelo qual essa conservação foi imposta a esses prestadores. Só assim não será se a importância do objetivo prosseguido pelo acesso ultrapassar a do objetivo que justificou a conservação (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 165 e 166).

99 Ora, a argumentação do Governo dinamarquês visa uma situação em que o objetivo do pedido de acesso pretendido, a saber a luta contra a criminalidade grave, é de menor importância, na hierarquia dos objetivos de interesse geral, do que o que justificou a conservação, a saber a salvaguarda da segurança nacional. Autorizar, em tal situação, um acesso aos dados conservados iria contra essa hierarquia dos objetivos de interesse geral recordada no número anterior e nos n.os 53, 56, 57 e 59 do presente acórdão.

100 Além disso, e sobretudo, em conformidade com a jurisprudência recordada no n.º 65 do presente acórdão, os dados de tráfego e os dados de localização não podem ser objeto de uma conservação generalizada e indiferenciada para efeitos da luta contra a criminalidade grave e, portanto, um acesso a esses dados não pode ser justificado para esses mesmos efeitos. Ora, quando esses dados foram excecionalmente conservados de maneira generalizada e indiferenciada, para efeitos de salvaguarda da segurança nacional contra uma ameaça que se revela real e atual ou previsível, nas condições referidas no n.º 58 do presente acórdão, as autoridades nacionais competentes em matéria de investigações penais não

podem aceder aos referidos dados no âmbito de ações penais, sob pena de privar de qualquer efeito útil a proibição de proceder a essa conservação para efeitos da luta contra a criminalidade grave, recordada no referido n.º 65.

101 Tendo em conta todas as considerações precedentes, há que responder à primeira, segunda e quarta questões que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

— uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

— uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

— uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

— uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem;

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

Quanto à terceira questão

102 Com a sua terceira questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º I, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional.

103 A título preliminar, importa recordar que, embora caiba ao direito nacional determinar as condições em que os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes o acesso aos dados de que dispõem, uma legislação nacional deve, para satisfazer a exigência de proporcionalidade, conforme recordada no n.º 54 do presente acórdão, prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente esses dados contra os riscos de abuso [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 48 e jurisprudência referida].

104 Em especial, uma legislação nacional que regula o acesso das autoridades competentes a dados de tráfego e a dados de localização conservados, adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, não se pode limitar a exigir que o acesso das autoridades aos dados responda à finalidade prosseguida por essa legislação, mas deve igualmente prever as condições materiais e processuais que regem essa utilização [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 49 e jurisprudência referida].

105 Assim, quando um acesso geral a todos os dados conservados, independentemente de qualquer ligação, no mínimo indireta, com o objetivo prosseguido, não puder ser considerado limitado ao estritamente necessário, a legislação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições em que o acesso aos dados em causa deve ser concedido às autoridades nacionais competentes. A este respeito, tal acesso só poderá, em princípio, ser concedido, em relação com o objetivo de luta contra a criminalidade, aos dados de pessoas que se suspeita estarem a planear, a cometer ou terem cometido uma infração grave ou, ainda, estarem envolvidas de uma maneira ou de outra nessa infração. Todavia, em situações especiais, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública sejam ameaçados por atividades terroristas, o acesso aos dados de outras pessoas poderá igualmente ser concedido quando existam elementos objetivos que permitam considerar que esses dados poderiam, num caso concreto, contribuir efetivamente para a luta contra essas atividades [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 50 e jurisprudência referida].

106 A fim de garantir, na prática, o pleno respeito destas condições, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 51 e jurisprudência referida].

107 Esse controlo prévio exige, designadamente, que o órgão jurisdicional ou a entidade administrativa independente encarregada de o efetuar disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação dos diferentes interesses e direitos em causa. No que respeita, mais especificamente, a um inquérito penal, tal controlo exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por

um lado, os interesses legítimos ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito [Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 52].

108 Quando esse controlo não é efetuado por um órgão jurisdicional, mas por uma entidade administrativa independente, esta deve gozar de um estatuto que lhe permita agir, quando desempenha as suas missões, de maneira objetiva e imparcial, devendo, para esse efeito, estar ao abrigo de qualquer influência externa. Assim, a exigência de independência que deve satisfazer a entidade encarregada de exercer o controlo prévio impõe que esta tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo a que a referida entidade possa exercer esse controlo de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, a exigência de independência implica que a autoridade encarregada desse controlo prévio, por um lado, não esteja implicada na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.ºs 53 e 54].

109 Assim, o Tribunal de Justiça considerou, nomeadamente, que não se pode reconhecer a um Ministério Público que dirige o processo de inquérito e exerce, sendo caso disso, a ação pública, a qualidade de terceiro em relação aos interesses legítimos em causa, uma vez que o mesmo não tem por missão decidir com total independência um litígio, mas submetê-lo, sendo caso disso, ao órgão jurisdicional competente, enquanto parte no processo que exerce a ação penal. Por conseguinte, esse Ministério Público não está em condições de efetuar o controlo prévio dos pedidos de acesso aos dados conservados [v., neste sentido, Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.ºs 55 e 57].

110 Por último, o controlo independente exigido em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58 deve ser efetuado previamente a qualquer acesso aos dados em causa, salvo em caso de urgência devidamente justificada, devendo, nesse caso, o controlo ser efetuado em prazos curtos. Com efeito, um controlo posterior não permitiria responder ao objetivo de um controlo prévio, que consiste em impedir que seja autorizado um acesso aos dados em causa que ultrapasse os limites do estritamente necessário [v., neste sentido, Acórdãos de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 189, e de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, EU:C:2021:152, n.º 58].

111 No caso em apreço, resulta, desde logo, do pedido de decisão prejudicial que a Lei de 2011 atribui a um agente de polícia, cuja posição não seja inferior à de superintendente chefe, a competência para exercer o controlo prévio dos pedidos de acesso aos dados que emanam dos serviços de investigação policial e para solicitar aos prestadores de serviços de comunicações eletrónicas que lhe comuniquem os dados por eles conservados. Na medida em que este agente não tem a qualidade de terceiro em relação a esses serviços, não cumpre as exigências

de independência e de imparcialidade recordadas no n.º 108 do presente acórdão, não obstante a circunstância de ser assistido nessa missão por uma unidade da polícia, neste caso, a TLU, que beneficia de um certo grau de autonomia no exercício da sua missão.

112 Em seguida, embora seja verdade que a Lei de 2011 prevê mecanismos de fiscalização *ex post* da decisão do agente de polícia competente, sob a forma de um procedimento de reclamação e de um processo perante um juiz encarregado de verificar a aplicação das disposições da referida lei, resulta da jurisprudência recordada no n.º 110 do presente acórdão que uma fiscalização exercida *ex post* não pode substituir a exigência, recordada no n.º 106 do presente acórdão, de controlo independente e, salvo caso de urgência devidamente justificada, prévio.

113 Por último, a Lei de 2011 não prevê critérios objetivos que definam com precisão as condições e as circunstâncias em que deve ser concedido às autoridades nacionais o acesso aos dados, uma vez que o agente de polícia encarregado do tratamento dos pedidos de acesso aos dados conservados é o único competente, conforme confirmou a Irlanda na audiência, para apreciar as suspeitas que recaem sobre as pessoas em causa e a necessidade de um acesso aos dados relativos a estas últimas.

114 Por conseguinte, há que responder à terceira questão que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º l, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional.

Quanto à quinta e sexta questões

115 Com a quinta e sexta questões, que devem ser examinadas em conjunto, o órgão jurisdicional de reenvio pretende saber, em substância, se o direito da União deve ser interpretado no sentido de que um órgão jurisdicional nacional pode limitar no tempo os efeitos de uma declaração de invalidade, que lhe incumbe por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz da Carta.

116 Resulta das informações fornecidas pelo órgão jurisdicional de reenvio que a legislação nacional em causa no processo principal, a saber, a Lei de 2011, foi adotada para transpor para o direito nacional a Diretiva 2006/24, que foi posteriormente declarada inválida pelo Tribunal de Justiça no seu Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238).

117 Além disso, o órgão jurisdicional de reenvio salienta que, embora o exame da admissibilidade dos meios de prova baseados em dados conservados ao abrigo da Lei de 2011 e invocados contra G.D. no âmbito do processo penal incumba ao juiz penal, é, no entanto, a ele que cabe decidir, no âmbito da ação cível, sobre a validade das disposições em causa desta lei e sobre os efeitos no tempo de uma declaração de invalidade das mesmas. Assim, embora a única questão que se coloca ao órgão jurisdicional de reenvio seja a da validade das disposições da Lei

de 2011, o referido órgão jurisdicional considera, todavia, necessário interrogar o Tribunal de Justiça quanto à incidência de uma eventual declaração de invalidade sobre a admissibilidade dos meios de prova obtidos através da conservação generalizada e indiferenciada dos dados que esta lei permitiu.

118 A título preliminar, importa recordar que o princípio do primado do direito da União consagra a prevalência do direito da União sobre o direito dos Estados-Membros. Este princípio impõe, assim, a todas as instâncias dos Estados-Membros que confiram pleno efeito às diferentes disposições do direito da União, não podendo o direito dos Estados-Membros afetar o efeito reconhecido a essas disposições no território dos referidos Estados. Por força deste princípio, na impossibilidade de proceder a uma interpretação da legislação nacional conforme com as exigências do direito da União, o juiz nacional encarregado de aplicar, no âmbito da sua competência, as disposições do direito da União tem a obrigação de garantir o pleno efeito das mesmas, não aplicando, se necessário e por sua própria iniciativa, qualquer disposição contrária da legislação nacional, mesmo que posterior, sem ter de pedir ou de esperar pela sua revogação prévia por via legislativa ou por qualquer outro procedimento constitucional [v., neste sentido, Acórdãos de 15 de julho de 1964, Costa, 6/64, EU:C:1964:66, pp. 1159 e 1160; de 19 de novembro de 2019, A. K. e o. (Independência da Secção Disciplinar do Supremo Tribunal), C-585/18, C-624/18 e C-625/18, EU:C:2019:982, n.os 157, 158 e 160; e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 214 e 215].

119 Só o Tribunal de Justiça pode, a título excecional e com base em considerações imperiosas de segurança jurídica, conceder uma suspensão provisória do efeito de exclusão exercido por uma regra do direito da União relativamente ao direito nacional a ela contrário. Essa limitação no tempo dos efeitos da interpretação deste direito dada pelo Tribunal de Justiça apenas pode ser concedida no próprio acórdão que decide sobre a interpretação pedida. O primado e a aplicação uniforme do direito da União ficariam comprometidos se os órgãos jurisdicionais nacionais pudessem, ainda que a título provisório, dar primazia às disposições nacionais sobre o direito da União (Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.os 216, 217 e jurisprudência referida).

120 É certo que o Tribunal de Justiça considerou, num processo em que estava em causa a legalidade de medidas adotadas em violação da obrigação, imposta pelo direito da União, de ser efetuada uma avaliação prévia das incidências de um projeto sobre o ambiente e sobre um sítio protegido, que um órgão jurisdicional nacional pode, se o direito interno o permitir, excecionalmente manter os efeitos de medidas se essa manutenção for justificada por considerações imperiosas ligadas à necessidade de afastar uma ameaça real e grave de rutura do abastecimento em eletricidade do Estado-Membro em causa, à qual não se pode fazer face por outros meios e alternativas, nomeadamente no âmbito do mercado interno, só podendo a referida manutenção abranger o período de tempo estritamente necessário para sanar essa ilegalidade (v., neste sentido, Acórdão de 29 de julho de 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, n.os 175, 176, 179 e 181).

121 Ora, contrariamente à omissão de uma obrigação processual como a avaliação prévia das incidências de um projeto, que se inscreve no domínio específico da proteção do ambiente, uma violação do artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não pode ser objeto de regularização por meio de um procedimento comparável ao mencionado no número anterior (v., neste sentido, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 219).

122 Com efeito, a manutenção dos efeitos de uma legislação nacional como a Lei de 2011 significaria que esta legislação continua a impor aos prestadores de serviços de comunicações eletrónicas obrigações contrárias ao direito da União e que comportam ingerências graves nos direitos fundamentais das pessoas cujos dados foram conservados (v., por analogia, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 219).

123 Por conseguinte, o órgão jurisdicional de reenvio não pode limitar no tempo os efeitos de uma declaração de ilegalidade que lhe compete, por força do direito nacional, da legislação nacional em causa no processo principal (v., por analogia, Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 220).

124 A este respeito, conforme salientou o advogado-geral, em substância, no n.º 75 das suas conclusões, a circunstância de esta legislação nacional ter sido adotada para efeitos de transposição para o direito nacional da Diretiva 2006/24 não é pertinente, dado que, em razão da invalidação desta diretiva pelo Tribunal de Justiça, invalidação cujos efeitos remontam à data da sua entrada em vigor (v., neste sentido, Acórdão de 8 de fevereiro de 1996, FMC e o., C-212/94, EU:C:1996:40, n.º 55), a validade desta legislação nacional deve ser apreciada pelo órgão jurisdicional de reenvio à luz da Diretiva 2002/58 e da Carta, conforme interpretadas pelo Tribunal de Justiça.

125 No que respeita, mais especificamente, à interpretação da Diretiva 2002/58 e da Carta adotada pelo Tribunal de Justiça nomeadamente nos seus Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970), e de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), há que recordar que, segundo jurisprudência constante, a interpretação que o Tribunal de Justiça faz de uma regra do direito da União, no exercício da competência que lhe é conferida pelo artigo 267.º TFUE, clarifica e precisa o significado e o alcance dessa regra, tal como deve ou deveria ter sido entendida e aplicada desde a data da sua entrada em vigor. Daqui decorre que a regra assim interpretada pode e deve ser aplicada a relações jurídicas surgidas e constituídas antes do acórdão que se pronuncia sobre o pedido de interpretação, se estiverem também reunidas as condições que permitem submeter aos órgãos jurisdicionais competentes um litígio relativo à aplicação da referida regra (Acórdão de 16 de setembro de 2020, Romenergo e Aris Capital, C-339/19, EU:C:2020:709, n.º 47 e jurisprudência referida).

126 A este respeito, importa ainda precisar que não se procedeu a uma limitação no tempo dos efeitos da interpretação adotada nos Acórdãos de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970), e de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), pelo que, em conformidade com a jurisprudência recordada no n.º 119 do presente acórdão, a mesma não pode ter lugar num acórdão do Tribunal de Justiça posterior a eles.

127 Por último, no que respeita à incidência da constatação da eventual incompatibilidade da Lei de 2011 com a Diretiva 2002/58, lida à luz da Carta, na admissibilidade das provas apresentadas contra G.D. no âmbito do processo penal, basta remeter para a jurisprudência do Tribunal de Justiça a ela relativa, em particular para os princípios recordados nos n.os 41 a 44 do Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152), do qual decorre que esta admissibilidade cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

128 Tendo em conta as considerações precedentes, há que responder à quinta e sexta questões que o direito da União deve ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz da Carta. A admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

Quanto às despesas

129 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara:

1) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,

— uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

— uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

— uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

— uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem,

desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

2) O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma legislação nacional ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, assistido por uma unidade instituída no âmbito da polícia que goza de um certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional.

3) O direito da União deve ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz da Carta dos Direitos Fundamentais. A admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

Comunicado de Imprensa n.° 68/22 do Tribunal de Justiça, Luxemburgo, de 28 de abril de 2022, Acórdão no processo C-319/20 Meta Platforms Ireland

As associações de defesa dos consumidores podem intentar ações coletivas contra violações da proteção dos dados pessoais

Esse tipo de ações pode ser intentado independentemente da violação concreta do direito à proteção dos dados de um titular e sem mandato desse titular para o efeito.

A Meta Platforms Ireland, anteriormente Facebook Ireland, é responsável pelo tratamento de dados pessoais dos utilizadores da rede social em linha Facebook na União.

A Federação das Associações de Consumidores dos Estados Federados (Alemanha) intentou uma ação inibitória contra a Meta Platforms Ireland, por considerar que esta violou, no contexto da colocação à disposição dos utilizadores de jogos gratuitos fornecidos por terceiros[255], as regras relativas à proteção dos dados pessoais, à luta contra a concorrência desleal e à proteção dos consumidores.

O Supremo Tribunal de Justiça Federal (Alemanha) observa que a ação da Federação é procedente mas tem dúvidas quanto à sua admissibilidade.

Com efeito, este órgão jurisdicional interroga-se sobre a questão de saber se uma associação de defesa dos interesses dos consumidores, como a Federação, ainda tem, desde a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (RGPD)[256], legitimidade ativa para intentar uma ação nos tribunais cíveis por violações deste regulamento e independentemente da violação de direitos concretos de determinados titulares dos dados e sem mandato destes. Além disso, observa que se pode inferir do RGPD que incumbe principalmente às autoridades de controlo verificar a aplicação deste.

[255] Quando consulta o Centro de aplicações de alguns desses jogos, o utilizador é advertido de que a utilização da aplicação em causa permite à sociedade de jogos obter um determinado número de dados pessoais e a autoriza a proceder a publicações em nome deste utilizador. Esta utilização implica a aceitação pelo utilizador das condições gerais da aplicação e da sua política em matéria de proteção de dados.

[256] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1).

No seu acórdão hoje proferido, o Tribunal de Justiça constata que **o RGPD não se opõe a uma legislação nacional que permite a uma associação de defesa dos interesses dos consumidores agir judicialmente, sem que lhe tenha sido conferido um mandato para o efeito e independentemente da violação de direitos concretos dos titulares dos dados, contra o presumível autor de uma violação da proteção dos dados pessoais**, invocando a violação da proibição de práticas comerciais desleais, de uma lei em matéria de proteção dos consumidores ou da proibição da utilização de cláusulas contratuais gerais inválidas, **desde que o tratamento dos dados em causa seja suscetível de afetar os direitos conferidos por esse regulamento às pessoas singulares identificadas ou identificáveis.**

A título preliminar, o Tribunal salienta que o RGPD procede a uma harmonização, em princípio completa, das legislações nacionais relativas à proteção dos dados pessoais. No entanto, determinadas disposições do RGPD conferem aos Estados-Membros a possibilidade de preverem regras nacionais adicionais que lhes deixam uma margem de apreciação quanto ao modo como essas disposições podem ser aplicadas, desde que as regras nacionais adotadas não prejudiquem o conteúdo e os objetivos do referido regulamento. A este respeito, eles têm nomeadamente a possibilidade de prever um meio processual de ação coletiva contra o presumível autor de uma violação da proteção dos dados pessoais, enunciando um determinado número de requisitos que devem ser respeitados.

O Tribunal sublinha, antes de mais, **que uma associação de defesa dos interesses dos consumidores, como a Federação, é suscetível de ser abrangida pelo conceito de «organismo com legitimidade ativa» na aceção do RGPD na medida em que prossegue um objetivo de interesse público** que consiste em garantir os direitos dos consumidores. Com efeito, a violação de regras relativas à proteção dos consumidores ou às práticas comerciais desleais pode estar relacionada com a violação das regras em matéria de proteção de dados pessoais.

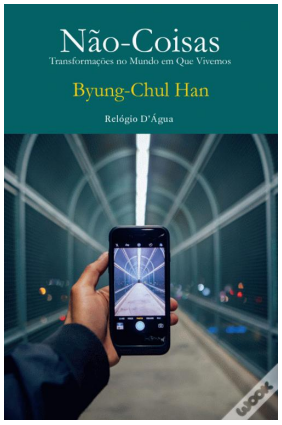
O Tribunal indica, em seguida, que a propositura de uma ação coletiva pressupõe que tal associação, independentemente de qualquer mandato que lhe tenha sido confiado, «considere» que os direitos do titular dos dados, previstos no RGPD, foram violados em virtude do tratamento dos seus dados pessoais, sem que seja necessário identificar, individual e previamente, o titular dos dados especificamente afetado pelo referido tratamento e alegar a existência de uma violação concreta dos direitos conferidos pelas regras em matéria de proteção de dados.

Tal interpretação é conforme com o objetivo prosseguido pelo RGPD, que consiste em **assegurar um nível elevado de proteção dos dados pessoais.**

Por último, segundo o Tribunal, o RGPD não se opõe a disposições nacionais que preveem o exercício de ações coletivas contra violações dos direitos conferidos por este regulamento através, se for caso disso, de regras que têm por objeto proteger os consumidores ou lutar contra práticas comerciais desleais.

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.

IV_Recensões



Não-Coisas: Transformações no Mundo em Que Vivemos

— Byung-Chul Han

Cristina Marai de Gouveia Caldeira[257]

Byung-Chul Han é um filósofo sul-coreano, professor da Universidade de Artes de Berlim onde leciona Filosofia e Estudos Culturais. É autor de uma dezena de ensaios de críticas à sociedade desde o trabalho à tecnologia. Na obra intitulada: *Não-Coisas, Transformações no mundo, em que vivemos*, o autor descreve o universo digital chamando a atenção para o menor apego da sociedade às coisas tangíveis, coisas que lhe conferia uma sensação de estabilidade. Refere ainda, que no presente, a nossa obsesão não se prende mais com coisas, mas ao invés estamos ávidos de informação e de dados. Vivemos na infoesfera, onde cada vez mais produzimos e consumimos informação, comunicamos e interagimos com infórmatos que agem e reagem como atores.

Byung-Chul Han defende que as "informações desenvolvem assim uma forma de vida sem estabilidade e duração" e, se por um lado, a infoesfera tem um lado emancipador, porque nos liberta de uma forma mais eficaz do trabalho árduo do que a esfera das coisas, por outro lado, condena-nos à prisão dos meios digitais. Mesmo no seu efeito emancipador, a digitalização propõe uma forma de vida, semelhante a um jogo, controlada por algoritmos, que reduz a capacidade de ação e autonomia da sociedade. Na sua critica à inteligência artificial, não deixa de afirmar que a tecnologia apenas processa factos previamente fixados, e que não atinge o contexto inicial no qual o pensamento tem a sua origem.

Segundo o autor, os algoritmos, tornam-se caixas negras, numa sociedade em que a informação já não a ilumina e não permite distinguir a verdade. O que realmente importa é o curto prazo, onde nada se aprofunda, onde o silêncio é substituído pelo ruido de uma comunicação permissiva, abrindo-se o caminho às *fake news*. Ainda assim, na era digital em que vivemos, o autor recorda Hannah Arendt e Heideguer, para salientar que a verdade possui a firmeza do ser e resiste a toda a manipulação.

---

[257] Pós-Doutorada na área da Propriedade Intelectual, Universidade Nova de Lisboa e investigadora de pós-doutoramento na Pontifícia Universidade Católica (PUCRS), Brasil. Doutorada em Direito na Especialidade em Ciências Jurídicas e Políticas pela Universidade Autónoma de Lisboa (UAL) e Programa Doutoral em Ciência Política na especialidade de políticas públicas, Universidade Católica Portuguesa. Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College. Colabora no Laboratório de Bioética no Hospital de Clínicas (RS Brasil), como investigadora na área de proteção de Tecnologia e Ensino Superior. Coautora de projetos de diplomas legais. Foi Vice-Reitora do IADE-U – Instituto de Arte, Design e Empresa – Universitário (2014-2015). É Diretora Executiva da Revista Privacy and Data Protection Magazine e Cocoordenadora Privacy and Data Protection Centre. Autora de várias publicações e participante regular em iniciativas públicas de Direito da Propriedade Intelectual e Proteção de Dados. Curriculum vitae: Ciência ID: 711B-87B9-6826. ORCID ID: https://orcid.org/0000-0001-6925-1877.