ISSN 1679-8694

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO

REVISTA DO TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO CAMPINAS/SP

Direção e coordenação da Escola Judicial
Repositório Oficial de Jurisprudência

Campinas n. 63 p. 1 - 332 jul./dez. 2023

AS DIVERSAS PERSPECTIVAS DA COLISÃO DE DIREITOS HUMANOS NA ERA DIGITAL: elementos para a compreensão e para a solução de aparentes antinomias

THE VARIOUS PERSPECTIVES OF THE COLLISION OF HUMAN RIGHTS IN THE DIGITAL AGE: elements for understanding and solution of antinomies

GEMIGNANI, Daniel[*]

Resumo: A era digital trouxe consigo a necessidade de se repensar a afirmação dos direitos humanos. As mudanças desencadeadas por essa nova realidade têm suscitado discussões que exigem a ressignificação de perspectivas forjadas para uma era ainda analógica, considerando as potencialidades do tratamento de dados. Nesse sentido, tem o presente trabalho a pretensão de apresentar novas perspectivas acerca da colisão entre direitos humanos, assim como elementos para a solução de aparentes antinomias.

Palavras-chave: Direitos humanos. Era digital. Antinomias.

Abstract: The digital age brought with it the need to rethink the human rights. The changes triggered by this new reality have given rise to discussions that require a new approach, considering the potential of data processing. In this regard, the present essay intends to present new perspectives on the competing human rights, as well as elements for the solution of antinomies.

Keywords: Human rights. Digital age. Antinomies.

[*]Procurador do Trabalho, Ministério Público do Trabalho (MPT). Bacharel em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Especialista em Auditoria Fiscal em Saúde e Segurança no Trabalho pela Universidade Federal do Rio Grande do Sul (UFRGS), e em Direito Aplicado ao Ministério Público do Trabalho pela Escola Superior do Ministério Público da União (ESMPU). Mestre em Direitos Humanos e Inclusão Social (Faculdade de Direito da Universidade de São Paulo - USP).

1 INTRODUÇÃO

A afirmação dos direitos humanos é tema que há tempos vem sendo objeto de estudo[1]. Sua análise, contudo, pode ser compreendida não apenas a partir de aspectos históricos, mas também da perspectiva daqueles que buscam sua efetivação. Nesse sentido é a distinção apresentada por Celso Lafer:

> 6. Na análise dos processos de asserção e mudança dos direitos do homem, na História, creio que é útil recorrer à distinção entre a perspectiva *ex parte populi* - a dos que estão submetidos ao poder - e a perspectiva *ex parte principis* - a dos que detêm o poder e buscam conservá-lo. Esta distinção que permeia a história do pensamento político não há de ser entendida como dicotomia do tipo dualista, ou seja, como cisão taxativa, graças à qual uma perspectiva exclui a outra. Trata-se, na verdade, de uma dicotomia do tipo pluralista que procura classificar, combinando, uma realidade complexa e uma permanente transformação. (LAFER, 2001, p. 125).

Essa distinção de perspectivas permite que se compreendam as disputas relativas ao tratamento de dados na era digital em suas mais diversas situações, como, *e. g.*, a definição de mínimos protetivos, quem deveria ser incumbido dessa proteção e a identificação das inúmeras colisões possíveis entre direitos, com suas respectivas repercussões. As novas tecnologias se apresentam, portanto, como catalisadoras de mudanças, notadamente ao evidenciarem colisões entre direitos[2] - alguns dos quais, inclusive, próprios da era digital[3].

---

[1]Nesse sentido, por todos, LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hannah Arendt. 1. ed., 4. reimpr. São Paulo: Companhia das Letras, 2001.

[2]Nesse sentido, CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. **International Review of Law, Computers & Technology**, Abingdon, v. 33, n. 1, p. 76-99, 2 Jan. 2019. Disponível em: http://dx.doi.org/10.1080/13600869.2019.1562604, p. 3; e GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism? Mapping attempts to craft an internet bill of rights. **Ssrn Electronic Journal**, Rochester, NY, Nov. 2015. Disponível em: http://dx.doi.org/10.2139/ssrn.2687120. Acesso em: 14 ago. 2021, p. 2-3.

[3]"Indeed, there are a number of areas of controversy or confusion in the application of human rights law to cyberspace. **Some reflect ongoing debates within the human rights legal field that pre-exist the emergence of cyber**. These include questions concerning the relationship between human rights law and other international legal constructs such as the law of armed conflict, the territorial scope of application of human rights law obligations, and how to balance competing rights. But crucially, **there are also a number of unique features of cyberspace that exacerbate these persistent tensions, or that call for the specific engagement/adaptation of human rights law to address new circumstances**. Aspects of cyberspace that to some extent present new challenges include the mobility of data online, the amount of personal detail individuals render vulnerable through cyberspace, and the potential of acts emanating from or involving cyberspace

2 AS COLISÕES ENTRE DIREITOS HUMANOS NA ERA DIGITAL E OS PRESSUPOSTOS PARA A SOLUÇÃO DE APARENTES ANTINOMIAS

2.1 O necessário estabelecimento de padrões mínimos de decisão

A evolução científica trouxe, à já complexa questão da afirmação de direitos, a necessidade de se discutir sobre técnicas para a solução de aparentes antinomias entre direitos humanos, em especial quando se considera a miríade de atores envolvidos nessa questão[4]. A solução para as colisões entre direitos humanos, portanto, exige que se considerem as diversas perspectivas em que esses direitos são aplicados, no que se incluem os vários atores incumbidos dessa aplicação. Assim, nota-se emergir discussão sobre qual a conformação mais adequada para a tutela dos direitos na era digital.

Nesse contexto, pertinente é a menção ao caso M.C. *v.* Bulgaria (Application no. 39272/98)[5], em que a Corte Europeia de Direitos Humanos discutiu o dever da Bulgária de adotar patamar protetivo adequado, i. e., mínimo, considerando a Convenção Europeia de Direitos Humanos[6].

---

to cause grave disruption and harm to others. Indeed, **some legal scholars argue that there comes a point in which analogies and adaptations from the offline world are no longer feasible or helpful, and that international human rights law is not equipped to regulate cyber**" (RONA; AARONS, 2016, p. 503) (grifo nosso).

[4]"Such a perspective allows us to notice that **contemporary society is experiencing a new constitutional moment, whose main catalyst is the disruptive impact of digital technology** (see Mayer-Schönberger and Crowley 2006; Rodotà 2010; cf. Fischer-Lescano 2005; Slaughter and Burke-White 2002). As we will see more in depth in the second section, on the one hand, technological advancements have manifestly amplified the possibility for individuals to exercise their fundamental rights. One significant example of this is our unprecedented capability to communicate easily with each other, which was truly unforeseeable some decades ago. On the other hand, digital technology has also created new sources of threats to our fundamental rights. The increasing risks deriving from the processing of our personal data facilitated by the use of digital devices are exemplary. **Last, but not least, the rising relevance of digital technology in contemporary society has vested an extraordinary amount of power in non-state actors, such as the big multinational corporations and the transnational organisations which own, commercialise or manage this technology, to the detriment of traditional constitutional actors like nation states**" (CELESTE, 2019, p. 1-2) (grifo nosso).

[5]M.C. *v.* BULGARIA (coe.int). Disponível em: https://hudoc.echr.coe.int/eng?i=001-61521.

[6]"ARTIGO 3º Proibição da tortura. **Ninguém pode ser submetido a torturas, nem a penas ou tratamentos desumanos ou degradantes**. [...] ARTIGO 8º Direito ao respeito pela vida privada e familiar. 1. **Qualquer pessoa tem direito ao respeito da sua vida privada** e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções

Com efeito, após discorrer sobre normas e interpretações estrangeiras e internacionais afeitas à tutela da liberdade sexual, concluiu a Corte Europeia de Direitos Humanos, dentre outras questões, que a Bulgária não havia interpretado adequadamente os termos "use of force or threats" de modo a conferir proteção ativa à vítima, dissociando-se, assim, do padrão interpretativo estrangeiro e internacional.

No aspecto, destacam-se as seguintes razões de decidir:

> (b) O conceito moderno dos elementos configuradores do estupro e seu impacto na obrigação positiva dos Estados membros de prover proteção adequada às vítimas.
> [...]
> 155. A margem de apreciação das autoridades locais está circunscrita pelas disposições da Convenção [Europeia de Direitos Humanos]. Interpretando-as, e **considerando que a Convenção é principalmente um sistema de proteção dos direitos humanos, a Corte deve se atentar para as mudanças que vêm ocorrendo com os demais Estados convenentes, e ajustar-se, por exemplo, convergindo para esses novos parâmetros** [...].
> 156. [...]. Nas últimas décadas, contudo, vem se desvelando uma tendência na Europa e em outras partes do mundo no sentido de abandonar critérios formais e restritivos da legislação nessa matéria [...].
> **161. Independentemente da palavra utilizada pelo legislador, em inúmeros países a acusação envolvendo atos sexuais não consensuais, em qualquer circunstância, busca se assentar na interpretação dos termos legais relevantes ('coerção', 'violência', 'coação', 'ameaça', 'ardil', 'surpresa' ou outros) e a partir de uma perspectiva contextualizada e sensível das evidências**.
> [...]
> 166. A partir do exposto, **a Corte** [Búlgara] **é persuadida a não adotar um critério rígido para o julgamento de crimes sexuais, como prova de resistência física, sob pena de restar sem punição o crime praticado e, por**

penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. [...] ARTIGO 13º Direito a um recurso efectivo. **Qualquer pessoa cujos direitos e liberdades reconhecidos na presente Convenção tiverem sido violados tem direito a recurso perante uma instância nacional, mesmo quando a violação tiver sido cometida por pessoas que actuem no exercício das suas funções oficiais**. ARTIGO 14º Proibição de discriminação. O gozo dos direitos e liberdades reconhecidos na presente Convenção deve ser assegurado sem quaisquer distinções, tais como as fundadas no sexo, raça, cor, língua, religião, opiniões políticas ou outras, a origem nacional ou social, a pertença a uma minoria nacional, a riqueza, o nascimento ou qualquer outra situação" (TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM; CONSELHO DA EUROPA, 2013) (destaques para os pontos tidos por relevantes pela Corte Europeia de Direitos Humanos).

> **consequência, em risco à proteção efetiva da liberdade sexual dos indivíduos**. De acordo com os **parâmetros contemporâneos** nesta questão, **a obrigação positiva dos Estados membros, conforme os artigos 3º e 8º da Convenção Europeia de Direitos Humanos, caracteriza-se pela apenação de qualquer ato sexual não consensual, inclusive quando não caracterizada a resistência física da vítima**. (Grifo nosso).[7]

Ao final, decidiu a Corte:

> 170. A Corte observa que **o artigo 152, § 1º, do Código Criminal Búlgaro não menciona qualquer requisito relacionado à resistência física pela vítima ou define estupro de forma significativamente diferente daquele identificado em outros Estados membros**.

[7]Tradução livre. No original, p. 30-32 do acórdão: "While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is in principle within the State's margin of appreciation, effective deterrence against grave acts such as rape, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions. Children and other vulnerable individuals, in particular, are entitled to effective protection. [...] 153. On that basis, the Court considers that States have a positive obligation inherent in Articles 3 and 8 of the Convention to enact criminal-law provisions effectively punishing rape and to apply them in practice through effective investigation and prosecution. **(b) The modern conception of the elements of rape and its impact on the substance of member States' positive obligation to provide adequate protection**. 154. In respect of the means to ensure adequate protection against rape, States undoubtedly enjoy a wide margin of appreciation. In particular, perceptions of a cultural nature, local circumstances and traditional approaches are to be taken into account. **155. The limits of the national authorities' margin of appreciation are nonetheless circumscribed by the Convention provisions. In interpreting them, since the Convention is first and foremost a system for the protection of human rights, the Court must have regard to the changing conditions within Contracting States and respond, for example, to any evolving convergence as to the standards to be achieved** (see Christine Goodwin *v.* the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI). 156. The Court observes that, historically, proof of physical force and physical resistance was required under domestic law and practice in rape cases in a number of countries. **The last decades, however, have seen a clear and steady trend in Europe and some other parts of the world towards abandoning formalistic definitions and narrow interpretations of the law in this area** (see paragraphs 88-108 and 126-47 above). 157. Firstly, it appears that a requirement that the victim must resist physically is no longer present in the statutes of European countries. [...] **161. Regardless of the specific wording chosen by the legislature, in a number of countries the prosecution of non-consensual sexual acts in all circumstances is sought in practice by means of interpretation of the relevant statutory terms ('coercion', 'violence', 'duress', 'threat', 'ruse', 'surprise' or others) and through a context-sensitive assessment of the evidence** (see paragraphs 95 and 130-47 above). [...] 166. In the light of the above, **the Court is persuaded that any rigid approach to the prosecution of sexual offences, such as requiring proof of physical resistance in all circumstances, risks leaving certain types of rape unpunished and thus jeopardising the effective protection of the individual's sexual autonomy. In accordance with contemporary standards and trends in that area, the member States' positive obligations under Articles 3 and 8 of the Convention must be seen as requiring the penalisation and effective prosecution of any non-consensual sexual act, including in the absence of physical resistance by the victim**" (grifo nosso).

> [...].
> **171. O que é decisivo, contudo, é o significado conferido a palavras como 'força' e 'ameaças' ou outros termos utilizados em definições legais**. Por exemplo, em alguns sistemas legais, 'força' é interpretada para a caracterização do estupro como o simples fato de alguém praticar um ato sexual, ou outros atos libidinosos, com outra pessoa, sem seu consentimento. Como acima pontuado, **a despeito de diferenças nas definições legais, as Cortes de diferentes países vêm buscando desenvolver interpretação de modo a alcançar qualquer ato sexual não consentido**. (Grifo nosso).[8]

Logo, pode-se verificar que a era digital apresenta desafios às formas tradicionais de defesa de direitos, baseada em Estados nacionais com controle sobre os fatos ocorridos em seu território. As relações digitais, contudo, não se apresentam sob essa lógica, visto que se dão de forma **desterritorializada**. Não obstante isso, tem-se, ainda, dificuldade em se reconhecerem padrões protetivos **universais**, ante a ausência de clareza quanto à aceitação de que determinados níveis protetivos serão aceitos por todos. Portanto, das dificuldades existentes, conclui-se que a proteção dos direitos humanos na era digital exigirá que sejam forjados instrumentos de proteção adequados, i. e., um piso protetivo, minimamente controlado pelos Estados, e que sejam, também, padrões aceitos indistintamente, a fim de que eventuais colisões sejam solucionadas a partir de critérios uniformes.

2.2 O reconhecimento da existência de múltiplas instâncias de decisão

O estabelecimento de critérios mínimos de decisão com a fixação de padrões aceitos indistintamente, contudo, não é o único desafio apresentado pela era digital. No aspecto, nota-se emergir discussão acerca da forma como os direitos humanos deverão ser implementados,

[8]Tradução livre. No original, p. 33 do acórdão: "2. Application of the Court's approach. [...] **170. The Court observes that Article 152 § 1 of the Bulgarian Criminal Code does not mention any requirement of physical resistance by the victim and defines rape in a manner which does not differ significantly from the wording found in statutes of other member States**. As seen above, many legal systems continue to define rape by reference to the means used by the perpetrator to obtain the victim's submission (see paragraphs 74 and 88-100). **171. What is decisive, however, is the meaning given to words such as 'force' or 'threats' or other terms used in legal definitions**. For example, in some legal systems 'force' is considered to be established in rape cases by the very fact that the perpetrator proceeded with a sexual act without the victim's consent or because he held her body and manipulated it in order to perform a sexual act without consent. **As noted above, despite differences in statutory definitions, the courts in a number of countries have developed their interpretation so as to try to encompass any non-consensual sexual act** (see paragraphs 95 and 130-47)".

notadamente quando se considera a existência de diversos órgãos e instituições aptos a interpretá-los e efetivá-los. Nesse contexto, destaca-se o dever dos Estados de assegurar proteção[9] mesmo em áreas nas quais sua soberania se encontra ameaçada - por isso, deve este ser exercido na medida das suas efetivas possibilidades -, visto serem esses locais os mais propensos a violações dos direitos humanos no ambiente virtual[10].

Noutro giro, pertinente o reconhecimento da participação de organizações não estatais nessa tomada de decisões, considerando-se, pois, a eficácia horizontal dos direitos humanos. Cita-se, de forma exemplificativa, a aplicação dos direitos humanos pela **Internet Corporation for Assigned Names and Numbers** (ICANN), como a **Uniform Domain Names Disputes Resolution Policy** (UDRP), a fim de prevenir violações no uso do chamado *Domain Name System* (*DNS*)[11]. A perspectiva ampliada

[9]"In the **case of K.U. *v.* Finland**, interpreting the right to privacy under the ECHR, **the European Court of Human Rights (ECtHR) confirmed that States have positive obligations that apply to cyberspace**. [...] In finding a violation of the right to privacy, the ECtHR asserted that the object of the Article 8 right to privacy 'does not merely compel the State to abstain from [...] interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life'. These include 'a positive obligation inherent in Article 8 of the Convention [Convenção Europeia de Direitos Humanos] to criminalise offences against the person... and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution'. Thus, the Court found that it was a violation of petitioner's rights for the State not to compel the internet service provider to divulge to police the identity of the individual who placed the advertisement" (RONA; AARONS, 2016, p. 520) (grifo nosso).

[10]"Once the state loses effective control over part of its territory, it loses its law enforcement capacity as well as physical access to victims and the actual authors of the online human rights violations. Furthermore, **while cybercrimes and other online human rights violations can emanate from any place in the world, perpetrators are likely to find safe haven in areas outside the effective control of the territorial state where the latter cannot exercise its power of enforcement**" (BERKES, 2019, p. 204-205) (grifo nosso).

[11]Acerca do ICANN, veja-se: https://www.icann.org/. Sobre sua conformação atual, notadamente após sua desvinculação formal do Estados Unidos da América, veja-se: https://www.youtube.com/playlist?list=PLQziMT9GXafXm-5MHQ5YIcRNy5rdUCRhS. "Since the Domain Name System ('DNS'), which matches computer addresses to human-friendly domain names, is integral to the way in which we navigate the Internet, the human rights implications of the DNS are important due to their enormous scope and global reach. While the DNS is arguably a global public good, it is governed by a private, multi-stakeholder body, the Internet Corporation for Assigned Names and Numbers ('ICANN'). Lack of clarity about the nature of human rights obligations of private actors in Internet governance, coupled with their growing power and influence over public affairs, has long been one of the most pressing human rights issues in the digital age. [...] The UDRP was created in 1998 as an international legal framework for resolving disputes between trademark owners and domain name holders. Because of profound economic, political, and human rights implications, domain name disputes have been subject to substantial litigation, legislative action, and scholarly and civil society debate over the twenty years since the UDRP was created. [...] **In this context, important questions arise about what kind of ethical and legal obligations ICANN has to ensure that the upcoming UDRP reform is consistent with, and incorporates, the new Core Value of respect for internationally recognized human rights**" (ZALNIERIUTE, 2020, p. 199-200) (grifo nosso).

da aplicação dos direitos humanos e seu dever de proteção ativa pelos diversos atores envolvidos se apresentam como uma tendência inevitável, conquanto ainda controvertida:

> **Digital constitutionalism has been defined as the 'constellation of initiatives that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet'**. Traditionally, constitutionalist analyses, as well as human rights instruments, have focused on the exercise and limits of power by nation-states. **More recently, constitutionally inclined scholars and activists working on technology and Internet governance have also aspired to confront the practices of private companies and informal actors**. (ZALNIERIUTE, 2020, p. 202) (grifo nosso).[12]

As controvérsias decorrentes das colisões entre direitos humanos na era digital se refletem, ainda, naquelas discussões já identificadas quando da aplicação universal desses direitos, como, por exemplo, as relativas às normas a serem utilizadas[13], à coerência e à transparência das decisões decorrentes[14], e ao devido processo legal - como, *e. g.*, a possibilidade de recurso[15].

Logo, a efetivação dos direitos humanos na era digital, além de demandar soluções a partir de discussões há tempos conhecidas, como aquelas decorrentes da aplicação universal desses direitos e os conflitos daí decorrentes, exige, também, a identificação de novos mecanismos aptos a possibilitar o enfrentamento de discussões outrora desconhecidas, como as relacionadas à conformação dos órgãos e instituições dispostos a interpretá-los e efetivá-los, e seu dever de proteção ativa.

---

[12]Acerca das controvérsias na aplicação dos direitos humanos pelo ICANN, remeta-se ao capítulo 2 do texto, p. 210-211.

[13]"Overall, the lack of clear choice-of-law rules in the UDRP has resulted in the socalled 'U.S./ non-U.S. panels dichotomy', with two competing sets of rules: one set adhering to U.S. laws, and a second set comprised of *sui generis* UDRP rules developed by (largely) WIPO panels. This dichotomy may lead to different outcomes in the same circumstances, depending on the nationality of the parties to the dispute or the panelists deciding the dispute, which undermines the overall fairness, consistency, and predictability of the UDRP system" (ZALNIERIUTE, 2020, p. 226).

[14]ZALNIERIUTE, Monika. Reinvigorating human rights in internet governance: the UDRP procedure through the lens of international human rights principles. **Columbia Journal of Law & The Arts**, New York, NY, v. 43, n. 2, p. 197-235, 2020, p. 226-227.

[15]*Ibidem*, p. 229-231.

Razões de Estado e identificação das instâncias de decisão: conflitos entre as perspectivas *ex parte populi* e *ex parte principis*

A era digital trouxe, para além de discussões envolvendo a regulação material de uma nova realidade, desafios relacionados à jurisdição. De fato, "[b]ecause of the unique nature of cyberspace events we should have an existing model to help us view the cyber landscape" (STEPHENSON, 2019, p. 104)[16]. A disputa por um modelo aplicável, contudo, vem suscitando as mais diversas propostas[17]:

> **Traditional jurisdictional frameworks function in the physical world quite well**: (i) location where the company is headquartered, as a reference point of the laws that it must observe, and (ii) the location of the evidence, as the decisive parameter of the country which has jurisdiction over that piece of evidence. **But when the Internet and electronic data are involved, and specifically in the context of cross border data requests, the normative underpinnings that sustain these hooks are disrupted**. Accordingly, **it is remarkable how the disputes explored challenge these doctrines and battle for the ultimate decisive point of jurisdiction to lawfully compel the sought-after data**.
> [...]
> Looking at electronic data as things that can be regulated, a country has power to exercise prescriptive jurisdiction over data, under the principle enunciated above, when the data is within its territory. **The**

[16]A seguir, apresenta o autor o seguinte exemplo de especificidade trazida pela era digital: "In cyberspace, there are some interesting permutations of these possibilities. Perhaps the most significant of these is the differentiation between human-caused events and autonomous events. The most obvious of autonomous events in the physical world is the autonomous vehicle. Currently, in the United States, California, Nevada, Michigan and Florida have statutes relating to autonomous vehicles. The cyber version of an autonomous vehicle is an autonomous program referred to as a 'bot' (robot). An autonomous bot would be capable of learning and making decisions on its own based upon its programming rather than under the direct guidance of a human ('bot herder') or a command and control server. In the physical world, autonomous vehicles are manufactured by known entities and both the entity and the vehicles undergo examination and special licensing. If an autonomous event occurs involving the vehicle, there is a manufacturer and software developer that can be held accountable. In the cyber world it is very likely that the developer of a bot - usually a criminal hacker - will not be known. **So, we must divide the events in the cyber world into two broad categories: those under human control and autonomous events**. [...]" (STEPHENSON, 2019, p. 104-105) (grifo nosso).

[17]Cita-se, por exemplo, o denominado princípio de lótus, i. e., "The Lotus Principle is one of the most often cited principles in international jurisdictional disputes. It states simply that a sovereign State can act as it pleases as long as no other laws or treaties are contravened" (STEPHENSON, 2019, p. 121).

> **complicating factor is that bits can be stored anywhere; they are not ruled by the same physical constraints of atoms**. First, electronic data moves from place to place at a speed unparalleled by physical objects. Second, data is divisible: it can be broken into multiple parts and held in multiple locations. Third, data packets can be replicated and transmitted at the same time to multiple places: one merely requires the physical infrastructure that enables access to the Internet to undertake such actions. **Consequently, electronic data can be called 'multi-territorial' in a way that physical things cannot. The question posed is how this impacts the determination of prescriptive jurisdiction over electronic data**. (ABREU, 2018, p. 241-242) (grifo nosso).

Assim, propostas diversas vêm surgindo, como, por exemplo, a possibilidade de se considerar critérios diversos dos tradicionais a legitimar jurisdições concorrentes, ou a melhoria nos mecanismos existentes de cooperação internacional[18]. Noutro giro, há que se considerar as deletérias repercussões que podem advir da intervenção de jurisdições locais em entes/matérias internacionais, tendo-se em vista a inevitável contaminação das decisões a serem tomadas por interesses locais. Nesse sentido, tem-se o caso da ICANN, assim apresentado:

> Após a transição mencionada, foi criada uma segunda fase para sanar as controvérsias que não haviam sido solucionadas, fase essa que perdura até dias atuais. **O principal tema dessa segunda fase, reconhecidamente, é a questão da jurisdição**. Surgem, nesse contexto, as controvérsias acerca do futuro da ICANN, sendo de especial relevância as **controvérsias acerca do posicionamento dessa organização no âmbito do ordenamento jurídico norte-americano e as formas de impedir que este interfira na missão e nos processos da ICANN**. (SALIBA; BAHIA, 2019, p. 338-339) (grifo nosso).[19]

[18]ABREU, Jacqueline de Souza. Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience. **Revista de Informação Legislativa: RIL**, Brasília, v. 55, n. 220, p. 233-257, 2018, p. 248-249.

[19]Cite-se, ainda, ZALNIERIUTE, 2020, p. 226: "Overall, the lack of clear choice-of-law rules in the UDRP has resulted in the socalled 'U.S./non-U.S. panels dichotomy', with two competing sets of rules: one set adhering to U.S. laws, and a second set comprised of *sui generis* UDRP rules developed by (largely) WIPO panels. **This dichotomy may lead to different outcomes in the same circumstances, depending on the nationality of the parties to the dispute or the panelists deciding the dispute, which undermines the overall fairness, consistency, and predictability of the UDRP system**" (grifo nosso).

Vê-se, portanto, que a efetivação de direitos, notadamente dos direitos humanos, na era digital, é questão que perpassa, para além de discussões de direito material, por definições relacionadas à jurisdição. Interessante, no aspecto, é a ressalva metodológica de que, mesmo em se tratando de tema novo, "[p]erhaps more important to our research, it teaches that some apparent 'cyber cases' are, in fact, simple cases that can be addressed by settled law and legal norms" (STEPHENSON, 2019, p. 111)[20]; a busca por soluções aos conflitos entre direitos, portanto, pode demandar apenas a mera aplicação de respostas já existentes ou, na hipótese de problemas absolutamente novos, a criação de estruturas diferentes, disruptivas de qualquer outra já forjada.

Compreender a extensão das disputas na era digital, também, apresenta-se como essencial, seja porque eventuais respostas podem já existir, seja porque soluções podem demandar, na verdade, mudanças completas na forma de se pensar. Nessa toada, a discussão parece se centrar mais em se estabelecer um pressuposto normativo comum, ou mínimo, a partir do qual se dará a jurisdição, do que propriamente a definição de qual jurisdição deverá atuar, considerando-se as variadas, senão infinitas, combinações possíveis a justificar uma ou outra jurisdição, além das inevitáveis ressalvas relacionadas à defesa de interesses nacionais, à segurança do Estado e à soberania.

2.3 O tratamento de dados no centro da colisão de direitos

O novo modo de viver que exsurge da era digital trouxe consigo a necessidade de se interpretar os direitos humanos por "lentes tecnológicas"[21]. No aspecto, destaca-se a relevância do debate acerca da forma como as informações fornecidas e obtidas via internet devem ser tratadas, considerando, por um lado, as potencialidades da era digital e, por outro, o respeito aos direitos humanos - em suas mais variadas perspectivas e vertentes[22]:

[20]Conclusão alcançada pelo autor a partir da discussão do caso ProCD *v.* Zeidenberg.

[21]"Rightly, it has been said that today our fundamental rights can be read in a technological lens (ALVAREZ-CIENFUEGOS SUAREZ, 1999, p. 15-22), since the Internet facilitates their realization, as evidenced by online education initiatives, telemedicine, and electronic government" (SILVA, 2013, p. 17).

[22]"Although Internet Freedom represents progress, it has several limitations that make it inadequate. First, it is an approach that encapsulates concerns and prioritizes topics from a U.S. perspective and therefore lacks comprehensiveness. Second, it presents a narrow view of the relevance and synergies resulting from the interaction between the Internet and human rights. Third, it ignores that the Internet is an essentially private environment and therefore demands greater accountability from the private sector. Fourth, it ignores Internet governance. Fifth, it prioritizes market needs rather than the respect for human rights. [...]" (SILVA, 2013, p. 19).

> An Internet policy based on human rights **should be sustained by a global and comprehensive view of these rights, including civil and political rights, as much as social, economic, and cultural rights, including the right to development**. This policy **should empower individuals to effectively exercise their citizenship** in the digital environment and to be able to **participate in Internet governance, to establish clear responsibilities for private sector actors and to give preference to human rights over market demands**. (SILVA, 2013, p. 27) (grifo nosso).

A liberdade que se pretende através da internet, portanto, enseja a atuação de atores diversos - nacionais e internacionais, públicos e privados -, assim como a conciliação de perspectivas de atuação passivas e ativas. Essa estrutura, contudo, não inibe a ocorrência de choques entre direitos, assim como de abusos, sob o fundamento de se estar a exercer um direito fundamental.

Nesse contexto, traz María Rún Bjarnadóttir como exemplo os casos de publicização não consentida da intimidade (os denominados "*revenge porn*"[23]):

> Domestic calls for criminalization of the posting of revenge porn have been responded to with arguments for freedom of expression, worries that such means will contribute to a fragmented internet, and of a slippery slope of state interference online. Further, as revenge porn touches upon the balancing between competing human rights, the outsourcing of human rights assessment to private entities could become a point of discussion. (BJARNADÓTTIR, 2016, p. 205).

Nessa toada, vem se relegando a definição de limites aos casos práticos, buscando-se com isso evitar abusos, sem se afetar em demasia a liberdade digital - ainda que essa tendência não se mostre isenta de críticas:

[23]"The term revenge porn already poses a problem in terms of definition. Since introduced, the **term has been used** in public discourse as an acronym **for unconsented distribution of sexual or intimate material, often with personal information attached, and intent to inflict harm or damage to the person depicted. The material can have been produced with or without the consent or knowledge of the person depicted, it's sharing intended for personal use and not wider distribution, and with or without malicious intent of the distributor**. This wide variation in circumstances has led to criticism of the term claiming it to be misleading', resulting in calls for a different terminology such as, 'nonconsensual pornography' (NCP)" (BJARNADÓTTIR, 2016, p. 205) (grifo nosso).

> The Court has established that the protection provided to the freedom of expression under Article 10 does not apply to all expression as the Court has found that expressions that go against the fundamental values of the Convention will not be tested before the Court and will be deemed under the scope of Article 17, prohibiting the misuse of the Convention. Nevertheless the Court has stated that Article 10 protects not only 'information' or 'ideas' that are favorably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. **Thus, offensive expression can enjoy the protection of the Convention under Article 10, although it may be subject to limitations under paragraph 2, such as in the interests of the rights of others. Rights of others includes among other things the rights protected under Article 8. The borders between these rights have been tested in a number of cases regarding defamation and media freedom of expression**.
> [...]
> From the above it could be established that in states bound by the ECHR [24], **freedom of expression does not exist without limitations neither online nor offline. This indicates that there exists no such right as to exercise freedom of expression without any regard to a wider context such as the rights of others**. (BJARNADÓTTIR, 2016, p. 211) (grifo nosso).

O contexto em que o choque entre direitos se dá representa, portanto, fator essencial na análise acerca de qual valor deverá

[24] A Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), em seu artigo 13, parece trazer disposição semelhante: "ARTIGO 13. Liberdade de Pensamento e de Expressão. **1. Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e idéias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha**. [2.] O exercício do direito previsto no inciso precedente não pode estar sujeito à censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei a ser **necessária para assegurar: a) o respeito aos direitos ou à reputação das demais pessoas; ou b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral pública**. 3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de freqüências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de idéias e opiniões. 4. A lei pode submeter os espetáculos públicos à censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2º. **5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade, ao crime ou à violência**" (BRASIL, 1992) (grifo nosso).

prevalecer, i. e., se a liberdade daquele que se expressa na internet ou a intimidade da pessoa prejudicada por essa **suposta liberdade de expressão**. Referida perspectiva encerra a posição de que não há direitos humanos absolutos, mas, sim, direitos *prima facie*, que se conformam adequadamente em casos concretos[25]. Nada obstante sua construção a partir das experiências e preocupações referentes à liberdade na internet, fato é que a análise concreta de casos traz o risco de decisões casuísticas ou orientadas por apelos momentâneos, além de se mostrar desprovida de efeitos prospectivos, orientadores de condutas futuras. A busca por uma estrutura regulatória que assegure a liberdade na internet, portanto, parece não prescindir da fixação de parâmetros minimamente objetivos que orientem condutas futuras, ainda que estes possam resultar em fragmentação do sistema - fixação de um piso, a partir do qual conformações locais poderiam ser forjadas.

2.3.1 O estabelecimento de padrões mínimos para a regulação do tratamento de dados

A regulação do tratamento de dados se tornou tema central na era digital. De fato, "[t]he inconsistency in privacy perception around the world prompted little controversy until the era of cyberspace" (KULESZA, 2012, p. 748). Contudo, a consolidação do entendimento de que a proteção de dados é questão a ser endereçada não tem por resultado o estabelecimento de padrões de proteção mínimos, notadamente quando se verifica a existência de perspectivas diversas sobre o direito à privacidade e sobre como referido direito deveria ser protegido:

> The first challenge is the disaccord on the actual nature of the term. **Privacy is directly related to human rights and personal data protection in Europe, while in the United States and numerous other jurisdictions, it is perceived as an element of commercial enterprise**.
> [...]
> Privacy protection, as designed by data protection regulations and international human rights treaties, applies only to situations where individual privacy is threatened by government action or omission. If private actors threaten privacy protection, the civil

[25]Acerca das diversas teorias sobre os direitos fundamentais, sublinha-se a de SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2010.

> law protection of personal rights is often invoked to settle the dispute. (KULESZA, 2012, p. 748, 754) (grifo nosso).[26]

As diversas disputas relacionadas à privacidade e ao tratamento de dados vêm resultando na fragmentação das sistemáticas de proteção, naquilo que se identifica como "*splinternet*":

> **'Internet filtering' is a term used to describe the national practice of disabling access to certain online content that is deemed harmful by state authorities and is usually recognized as illegal by national laws**. Filtering policies are often criticized for a number of reasons. Internet censorship primarily limits the citizens' right to receive information. **It also creates a danger of particularization of the global network into smaller, national, wellfiltered systems where only some of the global content is available-only as much of it as national laws allow**. The vision of an effectively and extensively filtered Internet is sometimes pejoratively referred to as 'splinternet', a **term depicting the loss of the universality of the network (an Internet 'splintered' into separate local webs)**.
> **Typically used to control state residents' access to certain data and restrain their right to free speech (which includes the right to receive and impart information), Internet filtering may also be viewed as a limitation on individual rights, particularly the right to privacy**. (KULESZA, 2012, p. 762) (grifo nosso).

As soluções adotadas em razão da ausência de uma solução uniforme, contudo, suscitam discussões relacionadas, *inter alia*, à extensão

[26]A seguir, na p. 756: "Placing the right to privacy in the ambit of ECHR or the EU Charter of Fundamental Rights clearly defined it as a human right, and personal data is considered its primary designation. At the same time, in U.S. doctrine, personal data is perceived primarily as a commercial commodity. This perception is reflected by a strong and rapidly evolving personal data market. There is no uniform federal privacy regulation in the U.S because the government considers it an obstacle to developing free trade and e-commerce. Introducing federal privacy regulations would also be too complex considering the U.S. constitutional regime and the delegation of authority to the states. A unique model regulation developed with the help of the United States Department of Commerce guarantees the protection of few individual rights. **The document is aimed at aiding the market self-regulation by establishing a uniform standard for the protection of personal data. It is, therefore, quite different from the European model, which requires governments to take an active role in protecting state residents' privacy**. The inconsistency in privacy perception around the world prompted little controversy until the era of cyberspace. **With massive online interactions and personal data retention and exchange, the two different legal concepts of protecting privacy collided, and the need for their harmonization arose**" (KULESZA, 2012) (grifo nosso).

da proteção a ser conferida - e seus desdobramentos, como a autodeterminação informativa:

> Decisivo para a **concepção do direito à autodeterminação informativa é o princípio segundo o qual não mais existiriam dados insignificantes** nas circunstâncias modernas do processamento automatizado de dados. **O risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados tratados**. (MENDES, 2020, p. 11) (grifo nosso).

> Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais.[27]
> [...]
> Apenas sob o paradigma da interceptação, da escuta, do grampo - **situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias** - não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.
> O esforço a ser empreendido pela doutrina e pela jurisprudência seria, em nosso ponto de vista, basicamente o favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, ou seja, reconhecendo a íntima ligação que passam a ostentar os

[27]Nas p. 100-101, indica o autor os seguintes princípios norteadores da proteção de dados: "**a) Princípio da publicidade (ou da transparência)**, pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos; **b) Princípio da exatidão**: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade; **c) Princípio da finalidade**, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade); **d) Princípio do livre acesso**, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos; **e) Princípio da segurança física e lógica**, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado" (DONEDA, 2011) (grifo nosso).

> direitos relacionados à privacidade e à comunicação de dados. Desta forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa nas vicissitudes da Sociedade da Informação. (DONEDA, 2011, p. 95, 106) (grifo nosso).

O tratamento de dados, portanto, parece ensejar a ressignificação da privacidade, em especial quando se considera o contexto amplo e dinâmico criado pela era digital. A importância conferida aos dados pessoais e as possibilidades de seu tratamento, por certo, implicam que se interprete a privacidade sob perspectivas mais amplas que a tradicional. Nessa toada, admitir a necessidade de se reinterpretar os direitos da personalidade na era digital, em especial o direito à privacidade, não significa, por completo, sua desconsideração, mas sim admitir que o contexto no qual referidos direitos deve ser estudado mudou e, por isso, sua conformação deve também mudar.

2.3.2 O tratamento em massa de dados

O instantâneo intercâmbio de informações proporcionado pela evolução tecnológica, assim como a cada vez maior imprescindibilidade dos meios digitais para o desempenho das atividades quotidianas têm suscitado preocupações relacionadas ao conhecimento de dados pessoais. Com efeito, a possibilidade de tratamento de dados em massa - os quais são obtidos a partir de uma nova rotina de vida, na qual o fornecimento de informações se faz de modo constante - tem resultado na redução dos espaços de vida privado, seja a partir da possibilidade passiva de conhecimento de rotinas, comportamentos e, portanto, tendências, seja ativa, com o monitoramento, até mesmo *on-line*, de pessoas e comunidades inteiras. Se por um lado essas possibilidades ultrapassam barreiras cognitivas que eram instransponíveis na era **analógica**, permitindo o desenvolvimento de políticas públicas - inclusive de controle epidemiológico, considerando a pandemia causada pelo SARS-CoV-2[28] - e

[28]"In China, the government has required residents to download a smartphone app that tracks their movements and assigns them a color (red, yellow, or green) corresponding to their asserted public health risk. These color codes regulate access to 'subways, malls, and other public spaces'. The methodology by which an individual is color-coded is opaque, however, and the app 'also appears to share information with the police, setting a template for new forms of automated social control that could persist long after the epidemic subsides'. In South Korea, the government reportedly pushes cell phone alerts about infected individuals, sending detailed information including 'credit-card history, with a minute-to-minute record of their comings and goings from various local businesses'. That level of detail has led to infected individuals, being identified and suffering harassment. Israel has hastily repurposed mass location data secretly collected for counterterrorism purposes to track potentially infected individuals wherever they go. Meanwhile, in the United

de produtos ou serviços cada mais vez mais personalizados, por outro, têm suscitado preocupações relacionadas ao controle, muitas vezes de viés não democrático, de formas de agir e de pensar:

> **Despite the public health benefits touted by proponents, it is not clear that digital contact tracing can achieve its lavish claims, nor is it evident that it can do so without imposing disproportionate privacy harms**. Current technological limitations, as well as limitations in COVID-19 testing and support for quarantining identified contacts, undermine the efficacy of digital contact tracing efforts that its proponents seemingly take for granted. As for privacy, digital contact tracing efforts abroad already raise significant cause for concern. **These mass surveillance programs sweep up revealing location data indiscriminately. Although they are defended on grounds of emergency and the urgent need to contend with the present health crisis, experiences in those countries already reveal the potential for abuse. Moreover, our own history amply demonstrates that surveillance powers claimed on emergency grounds frequently remain after the emergency has passed, often morphing into tools of social control targeted against disfavored individuals and groups**. (RAM; GRAY, 2020, p. 4) (grifo nosso).

Interessante no aspecto é a discussão, baseada no contexto normativo norte-americano, acerca da possibilidade de vigilância massiva,

> [...] because this conduct does not intrude upon reasonable expectations of privacy [ou porque a coleta de informações se dá em um contexto] free to observe anyone's public movements or to access areas open to the public. (RAM; GRAY, 2020, p. 9).[29]

States, North and South Dakota have already issued an app for their residents, which gathers location data using cell towers, GPS, and Wi-Fi and stores those data on a centralized, private server. In all, according to one livetracking site, at least 53 contact tracing apps have already appeared across at least 29 countries. In the United States, the Supreme Court has held that individuals have the right to expect that 'the whole of their physical movements' will remain private. [Carpenter *v.* United States, 138 S. Ct. 2206, 2217 (2018)]. [...]" (RAM; GRAY, 2020, p. 2).

[29]"The Supreme Court has long allowed government agents to access through lawful means information voluntarily shared with third parties. For example, law enforcement can access information about a suspect's financial transactions through the suspect's bank or credit card servicer without worrying about the Fourth Amendment because this conduct does not intrude upon reasonable expectations of privacy. In a similar vein, government agents are free to observe anyone's public movements or to access areas open to the public without subjecting themselves to Fourth Amendment constraints. **Would either or both of these lines of cases-colloquially, the third-party**

A conclusão negativa dos autores dessa proposição se dá essencialmente em razão do detalhamento das informações que podem ser coletadas digitalmente - o que afastaria, portanto, as excludentes normalmente admitidas em contextos **analógicos** de coleta de informações -, e em razão da ausência de certeza quanto à extensão com a qual os dados coletados serão tratados[30] e sua finalidade.

Aliado às preocupações suscitadas, tem-se um componente adicional, relacionado à própria segurança do Estado. Esse componente, forte nas justificativas para a vigilância massiva nos Estados Unidos e na Rússia, foi objeto de análise pela doutrina, a qual, a partir de parâmetros externos a esses países, concluiu que:

> American and Russian systems of surveillance do not adequately respect the laws necessary in a democratic society, and therefore, must be reformed.
> [...]
> The court [Corte Europeia de Direitos Humanos] has heard several cases regarding surveillance as it pertains to the Convention [Convenção Europeia de Direitos Humanos]. Recently, in the cases of Roman Zakharov *v.* Russia and Szabo and Vissy *v.* Hungary, the court found surveillance systems in Russia and Hungary violate the Convention. (PALMISANO, 2017, p. 76, 83-84).

Conclui-se, assim, que a evolução proporcionada pela era digital tem suscitado discussões que exigem a ressignificação de perspectivas forjadas para uma era ainda **analógica**, considerando as potencialidades do tratamento de dados. Outrossim, diferentes perspectivas quanto à privacidade têm ensejado visões diferentes acerca da possibilidade de coleta massiva de dados, notadamente quando se consideram preocupações relacionadas à segurança do Estado. Essas preocupações, por certo,

---

and public observation doctrines-exempt epidemiological surveillance programs from Fourth Amendment scrutiny? Probably not" (grifo nosso). Os autores citam, em nota de rodapé, os seguintes casos: United States *v.* Miller, 425 U.S. 435 (1976); California Bankers Ass'n *v.* Shultz, 416 U.S. 21 (1974); United States *v.* Knotts, 460 U.S. 276 (1983), e California *v.* Greenwood, 486 U.S. 35 (1988) (*looking through trashcan placed at the curb for pickup is not a "search"*); Oliver *v.* United States, 466 U.S. 170 (1984) (*entering upon and examining "open fields" is not a search*).

[30]"In Carpenter, the Court held that neither the third-party nor the public observation doctrine could relieve law enforcement from the burden of securing a warrant before accessing cell site location data that are routinely gathered and aggregated by cellphone service providers for their own business purposes. The crux of the Court's reasoning was that location tracking reveals a host of intimate details about private associations and activities. The Court also worried that granting law enforcement unfettered access to this kind of data would facilitate programs of broad and indiscriminate search, threatening the right of the people to be secure against threats of arbitrary state power, and conjuring the specters of general warrants and writs of assistance that haunted the minds of the founding generation" (RAM; GRAY, 2020, p. 9).

representam desafios concretos à criação de um **piso** mundialmente aceito de proteção à privacidade na era digital, assim como à formatação de uma perspectiva efetivamente universal dos direitos humanos.

2.3.3 Colisão entre direitos humanos: o tradicional choque entre a liberdade e a intimidade

A liberdade é, por certo, um dos valores mais propalados e almejados na história humana. Se, por um lado, tem-se a liberdade como um valor a ser fomentado e protegido, por outro, pouco se sabe o que se quer, de fato, dizer com isso. As hoje denominadas *fake news* são, nesse contexto, fenômeno **supostamente** moderno a desafiar e acirrar a liberdade:

> An examination of the current landscape reveals two types of fake news: accidental and intentional.
> [...] Communication on the Internet lacks physicality, facilitating a 'disinhibition effect', which causes 'temporal synchrony'. In other words, communication on the Internet creates a wide space between actions and consequences. This chasm allows for Internet users to feel mentally divorced from the possible effects of their actions, especially those that seem statistically unlikely. Additionally, the anonymity afforded by the Internet allows individuals to skirt responsibility by posting anonymously or under a pseudonym. Compounded with the insouciance of the modem Internet user, is the allure of instant fame should a post go viral.
> [...]
> A single viral tweet from an ill-informed citizen did not generate the Columbian Chemicals explosion hoax; it was a 'highly coordinated disinformation campaign, involving dozens of fake accounts that posted hundreds of tweets for hours, targeting a list of figures precisely chosen to generate maximum attention'. The Columbian Chemicals disinformation campaign, and many other similar campaigns, have been traced back to a corporation in St. Petersburg, Russia, known as the Internet Research Agency, or less formally as Russia's 'troll farm'. (VOJAK, 2017, p. 130-132, 137).[31]

[31]Acerca da notícia: "C. Intentional - Fake News as an Agent of Chaos or Influence At 8:30 a.m. on September 11, 2014, the Director of the Office of Homeland Security and Emergency Preparedness for St. Mary Parish, Louisiana, Duval Arthur's phone rang. On the other end, was a person reporting an explosion at a local chemical processing plant, Columbia Chemical. Shortly after ending the conversation, Arthur received text messages and more phone calls claiming the same thing. On Twitter, hundreds of accounts reported the explosion, and '[t]he #ColumbianChemicals hashtag was full of eyewitness accounts of the horror'. From New York to Louisiana, journalists 'found their Twitter accounts inundated with messages about the disaster'" (VOJAK, 2017, p. 136).

A suposição de que "[...] democracy hinges on an informed citizenry, and the unfettered flow of information upon which citizens may make choices regarding their government" (VOJAK, 2017, p. 144) parece se assentar na ideia de que, informadas, as pessoas adotarão conclusões similares, quando na realidade pouco de lógico ou racional parece haver na criação ou no consumo de notícias. De outra banda, sustentar uma ampla liberdade de expressão, cujos eventuais efeitos deletérios apenas podem resultar em reparações, também se mostra insustentável, considerando a absoluta restrição a outros direitos humanos, notadamente aqueles relacionados à imagem e à honra[32]. Nesse contexto, surgem propostas visando ao tratamento da liberdade de expressão a partir de sua categorização:

> Commoditized speech (that is, speech which itself is a commodity) has value not for its ability to express an idea, but for its likelihood of being consumed. Much like a minnow stops being just a fish when put on the end of a hook, the value of commoditized speech comes from its ability to lure readers. The intent of commoditized speech is not to inform, opine, or express - it is to be thrust into the stream of clicks and create income for the author. The author is directly incentivized to create and publish content that is shocking and creates an urgent need to 'share'. Today, the law not only allows for this to happen, but also blindly protects the author's right to do so. Under the current First Amendment jurisprudence, fake news is indiscriminately protected. Under section 230 of the CDA, Facebook, Google, and anything else categorized as an ISP, are exempted from liability for the tortious behavior of its users. The recent barrage of fake news has forced some internet advertising companies to deny service to fake news publishers and suspended and delete social media accounts connected with fake news publishers. However, these

[32]As diferenças de perspectiva, em especial entre a Alemanha e os Estados Unidos, são retratadas por W. Brugger: "[...] Primeiro, na tradição americana, há mais confiança de que, em uma disputa entre boas e más opiniões, as boas prevalecerão. Segundo, o discurso ofensivo ou o discurso do ódio nos Estados Unidos teve, ocasionalmente, conseqüências libertadoras como, por exemplo, durante a era da luta pelos direitos civis e dos protestos contra a guerra do Vietnã; porém, a Alemanha e a Europa vêem o discurso do ódio exclusivamente ou primariamente como uma ferramenta de supressão ou aniquilação. Terceiro, diversamente dos alemães, os americanos não confiam no governo para selecionar as 'boas' opiniões das 'más' - uma conseqüência dessa postura é que a discriminação feita por atores governamentais com base em pontos de vista, mesmo se direcionada ao 'discurso do mal', é vista com suspeita e pode até ser caracterizada como 'pecado capital'. Quarto, afora a deferência à liberdade de expressão, o judiciário americano esforça-se para ver além do elemento 'ódio' no discurso suspeito, a fim de encontrar algum componente relacionado com o interesse público, mesmo se essa interpretação seja um tanto extensiva; não há tal tendência abrangente na Alemanha" (BRUGGER, 2007, p. 130).

> actions have all been spearheaded by the entities themselves in an attempt to rehab bad publicity in the wake of the 2016 presidential election.
> It has become glaringly obvious that the one-size-fits-all appeal of the First Amendment does not fit the amoeboid shape of the Internet. (VOJAK, 2017, p. 153).

A distinção entre liberdade de expressão e aquilo que se nominou por "*commoditized speech*" vem suscitando a possibilidade de empresas coibirem a prática desse **discurso-abusivo**, conferindo a um ente privado a atribuição/prerrogativa de dizer o que seria - e *a contrario sensu*, não seria - *fake news*[33], em algo como a repristinação da antiga figura do *gatekeeper*[34]. A assunção de que entes privados têm a obrigação de defender os direitos humanos (como consequência da eficácia horizontal dos direitos humanos), contudo, não parece implicar automaticamente na admissão de que tem o dever/direito de coibir

[33]"Following the 2016 U.S. presidential election many ISPs, including Twitter, Google, and Facebook, pledged to crackdown on fake news by creating 'trust indicators'. Many of these companies are creating algorithms to 'flag concerning articles'. The fact that there is a mathematical and scientifically grounded method by which fake news can be ferreted out and categorized as 'commoditized speech' is promising for potential regulation. [...] Article 10 of the ECHR includes the freedom for expression, the freedom to hold opinions, and receive and impart information. The second clause of Article 10 limits this freedom by allowing Member States to derogate from this right if 'prescribed by law and necessary for a democratic society'. The European Court of Human Rights (ECtHR) was established to enforce the ECHR, and has solidified itself as an astute arbiter of the freedom of expression since the early 1970s. 207 When confronted with claims of Article 10 violations, the ECtHR must balance the rights afforded in the Article with the limitations of Article 17. The effect of Article 17 is 'to withhold the benefit of the Convention's guarantees from those who wish to use them to further an objective contrary to the values protected by the Convention'. Article 17 has allowed the ECtHR to deny protection to clearly racist speech, hate speech, and speech denying the Holocaust. Unlike the First Amendment, the balancing of Article 10 and Article 17 of the ECHR creates a paradigm that aims to protect speech up to a certain point by reconciling the rights of an individual and the rights of the *hoi polloi*. This paradigm allows states to derogate from freedom of expression if the restriction is 'in accordance with the law' and meets the 'democratic necessity test'. 210 'The purpose of the 'democratic necessity test' is to ensure that any specific interference with rights is judged against the 'true', rather than the alleged, needs of a democratic society'" (VOJAK, 2017, p. 153-154).

[34]"The internet is revolutionary because it is the first speech technology that is not controlled by so-called 'gatekeepers'-individuals (*e. g.*, newspaper editors) who have the ability to decide whether and to what extent ordinary people can access that technology. **Throughout history, virtually all advances in speech technology came with gatekeepers who were able to control access to those technologies**. [...] The net effect was that, even though the press revolutionized speech technology, the elite (*e. g.*, governmental officials, newspapers, universities, and the rich who owned and controlled presses) were the primary beneficiaries of the new technology, and were the ones who were most able to use the printing press to disseminate their ideas. **If the gatekeepers of the print media refused a publication request, and the speaker could not afford to pay a printer to publish his ideas, the speaker was left with only more primitive methods of communication (*e. g.*, oral and handwritten methods)**. [...] Much of the internet's impact is due to the fact that **it is largely free of the traditional gatekeepers**" (WEAVER, 2020, p. 325-327, 330) (grifo nosso).

discursos[35]. Nessa toada, parece adequada a proposta que busca sustentar a regulamentação da liberdade de expressão não apenas a partir de uma solução baseada na "autorregulação regulada"[36], mas também no reconhecimento da importância de um tratamento multifacetado, do qual participam atores privados e entes internacionais e nacionais[37].

2.3.4 A discriminação na era digital: algoritmos como instrumento de identificação de comportamentos odiosos

O combate à discriminação pautada em fator de *discrimén* odioso é questão que vem atraindo grande atenção em razão da era digital. Trata-se, pois, de se discutir as repercussões do uso de algoritmos na tomada de decisões, as quais, não raras vezes, podem resultar em escolhas

[35]Nesse sentido, e de forma exemplificativa, as acusações em face da Facebook: DUFFY, Clare. CEO Mark Zuckerberg responds to the massive Facebook document dump. **CNN Business**, Atlanta, GA, 26 Oct. 2021. Disponível em: https://edition.cnn.com/2021/10/25/tech/facebook-earnings-q3/index.html. Acesso em: 26 out. 2021.

[36]"Isto é o que a teoria dos sistemas chamou de 'direito reflexivo' (TEUBNER, 1983; 1986; 1992), 'programas relacionais' (WILLKE, 1986) ou 'procedimentalização' (WITHÖLTER, 1986; 2011): trata-se de formas jurídicas que se distanciam do sistema político estatal e se implantam dentro da dinâmica autorreferente de outros sistemas (no caso, o sistema dos meios de comunicação digitais). O direito estatal busca não pré-definir as regras substantivas pelas quais os problemas serão resolvidos, mas meramente assegurar parâmetros procedimentais para a decisão a ser tomada na esfera privada. Trata-se, portanto, de uma alternativa (ou complemento) tanto à programação condicional (a definição direta de regras, com hipóteses e consequências estritas) quanto à programação finalística (a mera indicação de princípios ou objetivos de política pública, sem definição completa de seus meios)" (SABA *et al.*, 2021, p. 159-160).

[37]"Quanto à relação entre regulação estatal e autorregulação privada, pode-se abordá-la dentro de um espectro normativo que vai de posturas paternalistas a libertárias. A postura paternalista exigiria do direito estatal o controle total sobre a definição dos direitos, deveres, poderes e responsabilidades na esfera imaterial, com expectativas de que o Estado monopolizasse as sanções e protegesse o usuário diante das plataformas digitais. A postura libertária estimularia a governança liderada pelas plataformas, opondo-se a maiores intervenções governamentais sobre este mercado. Parece claro que garantir a liberdade de expressão contra a censura pública ou privada, e ao mesmo tempo reconhecer que há sempre uma regulação das expectativas normativas em jogo (pois cada plataforma traz uma incontornável definição do código, da programação e dos algoritmos), apresenta como solução a combinação de autorregulação e heterorregulação. Proibir a autorregulação e impor o direito estatal dentro de uma visão hierárquica monista e unidirecional é desconhecer a dinâmica 'anárquica' ou 'acêntrica' da nova configuração do sistema dos meios de comunicação. Liberar a pura autorregulação, por outro lado, é instituir um estado de natureza digital em que a concentração de poder econômico, informacional e político pelas plataformas digitais acaba por produzir um Leviatã descontrolado. O desenvolvimento da regulação das comunicações digitais por ordens jurídicas de diferentes escalas e domínios de validade - direito estatal--nacional, internacional, supranacional e transnacional-setorial - permite a mútua observação da incompletude de cada ordenação, a multiplicidade institucional para a canalização de denúncias e o encaminhamento de processos, vínculos de colaboração e concorrência entre corpos normativos, jurisprudenciais e arenas decisórias diversas (do Judiciário estatal às *cyber courts* privadas instituídas pelas próprias plataformas para arbitragem de conflitos entre elas e seus usuários)" (SABA *et al.*, 2021, p. 163-164).

discriminatórias, naquilo que alguns doutrinadores vêm chamando de **discriminação algorítmica**. Os algoritmos, contudo, diversamente de se constituírem em instrumentos de discriminação[38], parecem assumir o papel de verdadeiros reveladores dessas condutas, ante a possibilidade de se analisar os critérios programados para que as decisões sejam tomadas[39]:

> A defining preoccupation of discrimination law, to which we shall devote considerable attention, is **how to handle the resulting problems of proof**. Those problems create serious epistemic challenges, and they produce predictable disagreements along ideological lines.
> **Our central claim here is that when algorithms are involved, proving discrimination will be easier - or at least it should be, and can be made to be**. The law forbids discrimination by algorithm, and that prohibition can be implemented by regulating the process through which algorithms are designed. This implementation could codify the most common approach to building machine-learning classification algorithms in practice, and add detailed recordkeeping requirements. Such an approach would provide valuable transparency about the decisions and choices made in building algorithms - and also about the tradeoffs among relevant values.
> [...]
> It is tempting to think that human decision-making is transparent and that algorithms are opaque. We have argued here that with respect to discrimination, the opposite is true. **The use of algorithms offers far greater clarity and transparency about the ingredients and motivations of decisions, and hence far greater opportunity to ferret out discrimination**. (KLEINBERG *et al.*, 2018, p. 114, 163) (grifo nosso).

Interessante, no aspecto, é observar que mesmo critérios não necessariamente sensíveis podem esconder vieses[40], assim como o anúncio de posturas **supostamente** garantidoras de direitos pode resultar

[38]"Algorithms change the landscape - they do not eliminate the problem" (KLEINBERG *et al.*, 2018, p. 117).
[39]"[...] The real fear with algorithms is not what happens inside the algorithmic 'black box'. The training algorithm is in some sense the opposite of a black box; the algorithm summarizes the data according to the data given to it and the outcome that is specified. It is those human choices where the potential for problems, including discrimination, really arise" (KLEINBERG *et al.*, 2018, p. 137).
[40]"[...] is worth underlining this point: an algorithm that is formally blind to race or sex might be using a correlated proxy" (KLEINBERG *et al.*, 2018, p. 137).

em efeitos/incentivos deletérios[41]. A adequada regulação da questão, portanto, assume relevância, a fim de que sejam adotados mecanismos adequados de combate não só à discriminação direta, como à indireta[42]:

> Getting the proper regulatory system in place does not simply limit the possibility of discrimination from algorithms; it has the potential to turn algorithms into a powerful counterweight to human discrimination and a positive force for social good of multiple kinds. (KLEINBERG *et al.*, 2018, p. 115).

Vê-se, portanto, que os algoritmos, ao invés de singelamente representarem uma nova forma de discriminação - como uma releitura moderna do **ludismo** -, podem ser vistos como ferramentas voltadas justamente ao combate dessas condutas odiosas. Por certo, ao registrarem os padrões utilizados por seus programadores para tomada de decisões/tratamento de dados, possibilitam o rastreamento de condutas discriminatórias, diferentemente do que ocorre em decisões tomadas subjetivamente, sem qualquer registro de parâmetros. A afirmação dos direitos humanos, com a distinção entre decisões legítimas e discriminatórias, assim, parece não ter sido prejudicada pelas inovações da era digital, não obstante seja claro que as novas ferramentas tecnológicas disponibilizadas trazem consigo a necessidade de qualificação não só para seu uso, como para sua auditoria.

2.3.5 A regulamentação específica como forma de distinguir situações que demandam tratamento especializado

A transversalidade do uso dos dados pessoais destacada pelos avanços da era digital trouxe consigo desafios à sua regulação. Nesse contexto é que se pode compreender a insuficiência do Marco Civil da Internet e da Lei Geral de Proteção de Dados na regulação de todos os aspectos

[41]"Notice there can be some counter-intuitive results from this type of benchmarking. Suppose we have a firm that proudly announces it will no longer collect information on whether applicants have a prior criminal record. We compare that to the industry standard and find a similar firm in the same industry and local labor market that proudly announces they invest substantial resources in collecting information about prior criminal records that is as detailed and extensive as possible. Which firm do we imagine will be more likely to hire African-American applicants? **A growing body of research in economics suggests that the picture is complicated, in that suppressing information of one type (criminal record) can incentivize decision-makers to turn to other forms of information (race) in ways that may be overtly discriminatory**" (KLEINBERG *et al.*, 2018, p. 148) (grifo nosso).

[42]Nesse sentido, faz-se referência à Convenção 111 da Organização Internacional do Trabalho (OIT) sobre Discriminação em Matéria de Emprego e Profissão.

dessa realidade, seja pela extensão com que os dados pessoais são tratados nas mais diversas instâncias da sociedade[43], seja porque o acesso à informação representa perspectiva central na atuação regulatória/repressiva do Estado. Tratar da regulação dos dados pessoais, portanto, é buscar um adequado equilíbrio entre a proteção dos direitos humanos e a necessária atuação do Estado:

> **Dados pessoais como esses podem ser úteis para vários cibercrimes**, como estelionato e sequestro, que são consumados mediante o uso de técnicas de *phishing,* engenharia social e *identity theft* (falsa identidade). Podem servir para extorsão, perseguição obsessiva (*stalking*) e crimes contra a honra, mediante *doxxing*. Podem ser usados para uma infinidade de atos ilegítimos. **Por outro lado, o acesso a dados pessoais pelas chamadas *law enforcement agencies* servirá para a elucidação desses mesmos crimes e a prevenção de delitos violentos, inclusive o terrorismo, ou extremamente repugnantes, como a violência sexual contra menores na internet e por meio dela**.
> **É evidente que a proteção de dados dialoga com os direitos humanos em geral e com os da personalidade em particular**, entre eles o de não ser conhecido, o de manter os segredos da vida privada e o de ser esquecido. Relacionam-se, também, com a proteção do patrimônio, pois dados são um *asset* valioso no mercado, tanto para empresas legítimas quanto para

[43]Refere-se, de forma geral, às situações que demandariam tratamento específico, como aquelas descritas no art. 4º da Lei n. 13.709/2018: "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. § 2º É vedado o tratamento dos dados a que se refere o inciso III do *caput* deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do *caput* deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei n. 13.853, de 2019)" (BRASIL, 2018).

> criminosos em geral. Ademais, proteger dados pessoais significa impedir ou minorar a possibilidade de perseguições do Estado a pessoas por motivos ligados à religião, política, origem nacional ou orientação sexual, por exemplo. (ARAS, 2020, p. 22) (grifo nosso).

Assim, discutir a regulação do tratamento de dados traz consigo o debate acerca da forma como esses dados podem ser utilizados judicialmente, seja na conformação processual[44], seja quanto à sua utilização como meio de prova/defesa de direitos - notadamente na seara criminal[45]:

> Entre os diversos temas novos e difíceis da prova digital, destacam-se duas diferenças relevantíssimas, comparadas com os meios de provas tradicionais: uma ontológica e outra metodológica.
> Os elementos de prova relevantes, no caso da *computer forensics*, são conservados e transmitidos em linguagem não natural, mas digital. Assim, ainda que os dados digitais, em seu conteúdo informativo, possam ser diretamente percebidos por quem está em contato com eles, eles não possuem uma materialidade imediatamente constatável. Justamente por isso, para que produzam informação jurídica útil para a reconstrução histórica dos fatos, devem seguir os princípios informáticos. O **National Institute for Standard and Technology (NIST) distingue quatro fases da *computer forensics*: em suas fases de coleta dos dados, exame, análise e relatório**.
> [...]
> Por todas essas diferenças, quando comparadas com as tradicionais provas utilizadas no processo penal, em especial as chamadas fontes reais de provas, notadamente os documentos, a *digital evidence*, a produção da prova informática, exigiria uma intervenção legislativa, com regras legais próprias para a sua produção, admissão e valoração, sendo muitas vezes inadequadas as regras tradicionais sobre as provas clássicas do processo penal.
> [...] A cadeia de custódia em si deve ser entendi[d]a com[o] a sucessão encadeada de pessoas que tiveram contato com a fonte de prova real, desde que foi colhida,

[44] A título de exemplo, CHAVES JÚNIOR, José Eduardo de Resende. Processo em meio reticular-eletrônico: constitucionalismo dialógico e democracia hiper-real, no contexto dos megadados. **Jota Notícias Jurídicas**, São Paulo, 18 out. 2017.

[45] "[...] Porém, o marco legal brasileiro ainda é insuficiente para regular por inteiro a realidade jurídica dessa temática em nosso país porque falta uma lei que trate da proteção de dados para fins penais em geral" (ARAS, 2020, p. 23).

> até que seja apresentada em juízo. **É o conjunto de pessoas, uma após a outra (p. ex.: o investigador, o delegado de polícia, o perito, o escrivão do cartório etc.), que teve contato com tal coisa** (p. ex.: uma arma, um líquido, um tufo de fios de cabelo). Esse conjunto de pessoas e os momentos específicos em que cada uma delas teve contato com a evidência precisam ser registrados, isto é, documentados, para que se saiba, exatamente, quem teve contato com a coisa e quando isso ocorreu. (BADARÓ, 2021, p. 7-8) (grifo nosso).

Tem-se, portanto, que o desafio representado pelo tratamento de dados na era digital qualifica o debate acerca do direito ao acesso ao Poder Judiciário, outrora pautado nas tradicionais ondas preconizadas pela doutrina tradicional[46], na medida em que traz repercussões amplas na forma como o processo se desenvolverá, a impactar desde o **tempo do processo** - no que se inclui tanto o tempo de tramitação, quanto o necessário tempo de reflexão para a tomada de decisões -, passando pela forma como a prova pode ser apresentada e, por consequência, impugnada, até a relação entre os atores processuais, que passam a considerar os diversos fatos sociais, antes extraprocessuais[47], como passíveis de influência na solução a ser alcançada.

2.4 O direito à educação como instrumento apto à tutela de direitos humanos na era digital

O estudo da inclusão digital encerra ao menos duas perspectivas. Uma primeira, focada na "[...] disputa [...] entre corporações no avançado mercado de tecnologia", e outra que pretende dialogar mais proximamente com os "sujeitos, [às] práticas e [às] habilidades necessárias para o [...] desenvolvimento [da educação]" (ROSA, 2013, p. 33)[48]. A universalidade dos direitos humanos, nesse contexto, deve implicar na possibilidade de acesso efetivo aos meios digitais disponíveis, no que se inclui o saber utilizar as novas ferramentas e manejá-las para além das suas funcionalidades anunciadas - compreendendo-se, portanto, seus impactos, repercussões e o papel que cada integrante dessa nova

[46]Refere-se, por todos, à obra CAPPELLETTI, Mauro; GARTH, Bryant. **Acesso à justiça**. Tradução de Ellen Gracie Northfleet. Porto Alegre: Sérgio Antonio Fabris, 1988.

[47]Refere-se, aqui, ao brocado "*Quod non est in actis non est in mundo*".

[48]Na p. 34: "Os resultados da análise apontam que o atual estágio das TIC [tecnologias de informação e comunicação] e dos debates em torno delas levam à necessária **compreensão do campo da inclusão digital como uma dimensão da cidadania. Compreensão que se dá, fundamentalmente, por meio do conceito de letramento digital, cujo foco recai na qualidade do acesso e na autonomia dos sujeitos como alvos da ação governamental**" (ROSA, 2013) (grifo nosso).

realidade exerce. Trata-se, assim, de se cogitar da existência de um direito à efetiva inclusão digital:

> Em pesquisa bibliográfica, Mori (2011) identifica **três vertentes** de compreensão do conceito de inclusão digital: como 'acesso', **como 'alfabetização digital' e como 'apropriação de tecnologias'**. A primeira focaliza a distribuição de bens e serviços que garantam o acesso à infraestrutura e às TIC. Já na segunda vertente, o foco é colocado nas habilidades básicas em TIC, **que permitam ao indivíduo saber fazer uso delas, sendo, neste caso, o acesso aos meios físicos, bem como a alfabetização escolar, os requisitos necessários para se desenvolver. A terceira vertente defende um passo posterior à chamada alfabetização digital: além de saber usar, os indivíduos devem desenvolver uma compreensão dos novos meios que lhes permitam apropriar-se desses recursos para 'reinventar seus usos e não se constituir como meros consumidores'** [...]. (ROSA, 2013, p. 36) (grifo nosso).

A implementação desse direito, contudo, assume diferentes graus[49], os quais evidenciam formas diversas de se compreender a relação dos indivíduos com o Estado, e até mesmo daqueles entre si. Há, nesse contexto, posições que sustentam que o acesso à internet deve ser compreendido como um direito fundamental, sob "la premisa de que *Internet* es, a su vez, un instrumento extraordinario, un bien **público universal** cuyo acceso ha de estar garantizado a la ciudadanía" (LUCENA CID, 2014, p. 385); referida posição, contudo, parece confundir esse novo fenômeno e suas contingências com o conceito de direito, naquilo que:

> Anna Pintore (2001) llama los derechos insaciables, es decir, un apetito desmedido de la sociedad y sus grupos de presión por convertir todo a derechos: derecho al turismo, derecho a llorar, derecho a dormir etc. (TORRES ÁVILA, 2015, p. 49).

[49] "Por trás dessas escolhas, encontram-se duas concepções distintas: a universalização pressupõe que um dado bem ou serviço é direito de todos, e, como tal, deve ser garantido pelo Estado a toda população; já a focalização presume que o referido bem ou serviço concerne a uma capacidade de todos, sendo necessário provê-lo apenas aos que não podem obtê-lo por seus próprios meios" (ROSA, 2013, p. 39). A solução **focalizada**, apresentada pela autora, parece se assemelhar com a difusão dos chamados **orelhões** no Brasil do século passado, notadamente em época na qual o acesso aos telefones particulares não era universal, mas a necessidade por se comunicar se afigurava, cada vez mais, necessária.

A disputa acerca da extensão dos direitos digitais e suas consequentes colisões, portanto, parece se referir mais à compreensão dessa nova realidade sob a lógica dos direitos humanos do que propriamente à defesa de um direito amplo, em que todos os desdobramentos e contingências passam a ser caracterizados como direitos passíveis de serem reivindicados perante o Estado ou terceiros - olvidando-se, neste último caso, que os particulares muitas vezes representaram grupos de interesse específico e portam, em razão disso, vieses na forma como disponibilizam seus serviços digitais. Entender os direitos digitais como desdobramentos de direitos já assegurados, como o direito à educação, assim como um novo direito, a partir dos novos desafios apresentados pela internet, não parece implicar em reconhecê-los como algo universal - no sentido de ser a todos garantido a partir de uma pretensão jurídica -, mas, na realidade, em admiti-los como:

> [...] la expresión de una *praxis* política, con consecuencias jurídicas, como lo deja ver la interpretación misma que hacen los sistemas constitucionales de la democracia. (TORRES ÁVILA, 2015, p. 51).[50]

Nesse sentido, citam-se, de forma exemplificativa, as discussões hodiernamente travadas sobre a legitimidade de limitações aos meios digitais como forma de resguardo à intimidade, inclusive de trabalhadores no exercício de sua atividade laboral, assim como de **organizações de tendência** se negarem a acolher posições diversas daquelas que publicamente defendem. Essas discussões, contudo, parecem desconsiderar, por um lado, as especificidades ou contingências práticas, como a existência de atividades de risco, como as de motoristas e aeronautas, nas quais o **monitoramento** da fadiga por meios digitais, *e. g.*, parece se mostrar justificável, quando não impositivo, ante a necessária preservação do interesse da própria coletividade[51], e, de outra banda, que não apenas as

[50]Destaca-se, no aspecto, às p. 56-57: "En resumen, una visión estatalista atenta directamente contra las premisas de universalidad, imprescriptibilidad e inalienabilidad, pues se trata justamente de poner a disposición del Estado estas potestas. Sin embargo, en la actualidad esta tensión no se resuelve con un modelo puro de voluntad de Estado, sino que entran en juego diversos discursos que combinados explican cómo los Estados terminan reconociendo los derechos. Es decir, la visión del Estado como supremo ordenador no cuenta con un sustento de legitimidad a la luz de la teoría contemporánea de los derechos. De manera que el Estado, tiene múltiples mediaciones para poder actuar. La democracia, el derecho internacional público, las relaciones internacionales, los processos socioeconómicos y las condiciones políticas, son entre otros, quienes regulan, afectan y enfocan el esfuerzo estatal" (TORRES ÁVILA, 2015).

[51]"Ahora bien, los riesgos para los empleados derivados del uso de dispositivos digitales por el empleador tienen otras manifestaciones especialmente problemáticas cuando la intimidad de los trabajadores se ve amenazada por la utilización de dispositivos de videovigilancia, de grabación de

organizações de tendência encerram posições, visto que muitos dos entes privados que atuam com tecnologias da informação e comunicação (TIC) assim também o fazem, ainda que não publicamente. A proteção de direitos na era digital, portanto, não pode prescindir de uma efetiva inclusão digital, o que exige a compreensão de seus impactos, repercussões e o papel que cada integrante dessa nova realidade exerce.

3 CONCLUSÕES

A afirmação dos direitos humanos na era digital traz desafios variados, decorrentes das inúmeras colisões passíveis de ocorrer. As duas principais perspectivas de análise (*ex parte populi* e *ex parte principis*) revelam os pressupostos a partir dos quais as colisões ocorrem, mormente quando se considera não só a nova releitura que vem sendo exigida de direitos tradicionais, como a **identificação** de novos direitos.

A transversalidade e a universalidade dos direitos humanos, portanto, parecem indicar que a solução de eventuais colisões pode ser alcançada a partir da definição de critérios mínimos de proteção, a serem efetivados nas mais diversas instâncias de proteção admitidas. Trata-se, pois, de se assegurar que a pluralidade dos direitos humanos não seja tolhida por diferentes perspectivas, ao mesmo tempo em que não se admite a fixação de critérios protetivos inferiores a um padrão mínimo adequado. A definição desses padrões, contudo, não é algo ainda claro, nada obstante não se possa descartá-los pela simples dificuldade em sua definição, conforme evidenciam as hipóteses concretas de colisão, como aquelas envolvendo a intimidade. A era digital, portanto, trouxe consigo interessantes desafios, a exigir cada vez mais qualificação e conhecimento de todos, a fim de que a inclusão digital possa se dar de forma consciente, não só quanto às potencialidades desta nova era, como quanto às suas contingências.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Jurisdictional battles for digital evidence, MLAT reform, and the brazilian experience. **Revista de Informação Legislativa: RIL**, Brasília, v. 55, n. 220, p. 233-257, 2018.

sonidos o de geolocalización. La actuación de control del empleador para garantizar las obligaciones laborales requiere de reglas y limitaciones que modulen esta facultad de control empresarial para adecuarla a los usos y convenciones que amparan unas expectativas básicas de intimidad de los trabajadores" (RALLO LOMBARTE, 2020, p. 124).

ARAS, Vladimir Barros. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. *In*: ARAS, Vladimir Barros *et al*. (Coord.). **Proteção de dados pessoais e investigação criminal**. Brasília: Associação Nacional dos Procuradores da República (3ª Câmara de Coordenação e Revisão), Ministério Público Federal, 2020.

BADARÓ, Gustavo. Os *standards* metodológicos de produção da prova na prova digital e a importância da cadeia de custódia. **Boletim do IBCcrim**, São Paulo, n. 343, jun. 2021.

BERKES, Antal. Human rights obligations of the territorial state in the cyberspace of areas outside its effective control. **Israel Law Review**, Jerusalem, v. 52, n. 2, p. 503-530, July 2019.

BJARNADÓTTIR, M. R. Does the internet limit human rights protection: the case of revenge porn. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, Karlsruhe, v. 7, n. 3, p. 204-215, 2016.

BRASIL. Decreto n. 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. **DOU**, Brasília, 9 nov. 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **DOU**, Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.

BRUGGER, W. Proibição ou proteção do discurso do ódio? Algumas observações sobre o direito alemão e o americano. **Revista Direito Público**, Brasília, n. 15, p. 117-136, 2007.

CAPPELLETTI, Mauro; GARTH, Bryant. **Acesso à justiça**. Tradução de Ellen Gracie Northfleet. Porto Alegre: Sérgio Antonio Fabris, 1988.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. **International Review of Law, Computers & Technology**, Abingdon, v. 33, n. 1, p. 76-99, 2 Jan. 2019. Disponível em: http://dx.doi.org/10.1080/13600869.2019.1562604.

CHAVES JÚNIOR, José Eduardo de Resende. Processo em meio reticular-eletrônico: constitucionalismo dialógico e democracia hiper-real, no contexto dos megadados. **Jota Notícias Jurídicas**, São Paulo, 18 out. 2017.

COMPARATO, Fábio Konder. **A afirmação histórica dos direitos humanos**. 7. ed. São Paulo: Saraiva, 2009.

DEVA, Surya. The UN guiding principles' orbit and other regulatory regimes in the business and human rights universe: managing the interface. **Business and Human Rights Journal**, London, v. 6, n. 2, p. 336-351, June 2021. Disponível em: http://dx.doi.org/10.1017/bhj.2021.23.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Chapecó, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DUFFY, Clare. CEO Mark Zuckerberg responds to the massive Facebook document dump. **CNN Business**, Atlanta, GA, 26 Oct. 2021. Disponível em: https://edition.cnn.com/2021/10/25/tech/facebook-earnings-q3/index.html. Acesso em: 26 out. 2021.

GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism? Mapping attempts to craft an internet bill of rights. **Ssrn Electronic Journal**, Rochester, NY, Nov. 2015. Disponível em: http://dx.doi.org/10.2139/ssrn.2687120. Acesso em: 14 ago. 2021.

JACOBS, Nicholas. Federalism, polarization, and policy responsibility during Covid-19: experimental and observational evidence from the United States. ***Publius***: **The Journal of Federalism**, Oxford, v. 51, n. 4, p. 693-719, June 2021. Disponível em: http://dx.doi.org/10.1093/publius/pjab014.

KLEINBERG, Jon *et al*. Discrimination in the age of algorithms. **Journal of Legal Analysis**, Oxford, v. 10, p. 113-174, 2018. Disponível em: http://dx.doi.org/10.1093/jla/laz001.

KULESZA, Joanna. Walled gardens of privacy or binding corporate rules: critical look at international protection of online privacy. **University of Arkansas at Little Rock Law Review**, Little Rock, AR, v. 34, n. 4, p. 747-766, 2012.

KULESZA, Joanna; BALLESTE, Roy. Signs and portents in cyberspace: the rise of jus internet as a new order in international law. **Fordham Intell. Prop. Media & Ent. Law Journal**, New York, NY, v. XXIII, n. 4, p. 1311-1349, 2013.

LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hannah Arendt. 1. ed., 4. reimpr. São Paulo: Companhia das Letras, 2001.

LUCENA CID, Isabel Victoria. El derecho de acceso a internet y el fortalecimiento de la democracia. **Revista Internacional de Pensamiento Político**, Sevilla, v. 9, 2014.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828.

PALMISANO, M. The surveillance cold war: recent decisions of the European Court of Human Rights and their application to mass surveillance in the United States and Russia. **Gonzaga Journal of International Law**, Spokane, WA, v. 20, n. 2, p. 75-99, 2017.

RALLO LOMBARTE, A. Una nueva generación de derechos digitales. **Revista de Estudios Políticos**, Madrid, n. 187, p. 101-135, 2020.

RAM, Natalie; GRAY, David. Mass surveillance in the age of Covid-19. **Journal of Law and the Biosciences**, Durham, NC, v. 7, n. 1, p. 1-17, Jan. 2020. Disponível em: http://dx.doi.org/10.1093/jlb/lsaa023.

RONA, Gabor; AARONS, Lauren. State responsibility to respect, protect and fulfill human rights obligations in cyberspace. **Journal of National Security Law and Policy**, Washington, DC, v. 8, n. 3, p. 503-530, 2016.

ROSA, Fernanda Ribeiro. Inclusão digital como política pública: disputas no campo dos direitos humanos. **Sur International Journal on Human Rights**, São Paulo, n. 18, p. 33-54, 2013.

SABA, Diana Tognini *et al*. ***Fake news* e eleições**: estudo sociojurídico sobre política, comunicação digital e regulação no Brasil. Porto Alegre: Fi, 2021.

SALIBA, Aziz Tuffi; BAHIA, Amael Notini Moreira. A jurisdição da ICANN: desafios atuais e prospectivas futuras. **Revista de Direito Internacional**, Brasília, v. 16, n. 2, p. 334-345, 2019.

SILVA, A. J. Cerda. Internet freedom is not enough: towards an internet based on human rights. **Sur International Journal on Human Rights**, São Paulo, n. 18, June 2013.

SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2010.

STEPHENSON, P. R. International private law as model for private law jurisdiction in cyberspace. **Legal Issues Journal**, London, v. 7, n. 2, p. 103-134, 2019.

TORRES ÁVILA, Jheison. La fundamentación del derecho a la inclusión digital. **Revista Prolegómenos Derechos y Valores**, Bogotá, v. 18, n. 36, set. 2015. Disponível em: http://dx.doi.org/10.18359/dere.933.

TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM; CONSELHO DA EUROPA. **Convenção europeia dos direitos do homem**. Estrasburgo: COE, 2013. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por.

VOJAK, B. Fake news: the commoditization of internet speech. **California Western International Law Journal**, San Diego, CA, v. 48, n. 1, p. 123-158, 2017.

WEAVER, R. L. Free speech in an internet era. **University of Louisville Law Review**, Louisville, KY, n. 58, p. 325-348, 2020.

ZALNIERIUTE, Monika. Reinvigorating human rights in internet governance: the UDRP procedure through the lens of international human rights principles. **Columbia Journal of Law & The Arts**, New York, NY, v. 43, n. 2, p. 197-235, 2020.