NOVOS INSTRUMENTOS NÃO EFICAZES DE CONTROLE DAS TECNOLOGIAS DE COMUNICAÇÃO E INFORMAÇÃO

NEW NON-EFFECTIVE INSTRUMENTS FOR THE CONTROL OF COMMUNICATION AND INFORMATION TECHNOLOGIES

Afonso Paulo Albuquerque de Mendonça[1]

RESUMO

Para a coerente compreensão do problema é preciso entender as diferenças normativas na regulamentação das telecomunicações, das redes e da internet no Brasil. Necessária a diferenciação entre rede e internet. Aos olhos do leigo, a grande maioria dos usuários, a web é a parte que se acessa para os conteúdos veiculados na internet. O desconhecimento da área digital leva os juristas a apoiar a elaboração de novas leis. Ocorre que os algoritmos permitem que os sistemas cada vez mais aumentem em complexidade. É possível modelar uma arquitetura impulsionada pelo Estado e pelo mercado no sentido de uma regulamentação eficaz. Há de se adotar cautela ante a possibilidade de ameaças às liberdades.

Palavras-chave: Tecnologias. Internet. Redes. Controle. Autorregulação.

ABSTRACT

For a coherent understanding of the problem, it is necessary to understand the normative differences in the regulation of telecommunications, networks and the internet in Brazil. It is necessary to differentiate between network and internet. In the eyes of the layman, the vast majority of users, the web is the part that is accessed for the contents conveyed on the internet. Lack of knowledge of the digital area leads jurists to support the drafting of new laws. It turns out that algorithms allow systems to increasingly increase in complexity. It is possible to model a state- and market- driven architecture towards effective regulation. Caution must be exercised in the face of the possibility of threats to freedoms.

Keywords: Technologies. Internet. Networks. Control. Self-regulation.

[1] Mestrando em Direito Constitucional pelo Instituto Brasiliense de Direito Público (IDP). E-mail: **afonsopaulomendonca@hotmail.com**

1 INTRODUÇÃO

O enfrentamento normativo à evolução das tecnologias de comunicação e informação tem se mostrado ineficaz. A saber se as razões para tal perpassam pela necessidade da compreensão do funcionamento das redes e da internet. Em outro aspecto, de se identificar como poderia haver o controle pelo Estado e pelo mercado, se através do atual processo legislativo ou pela autorregulação do ciberespaço.

Em uma primeira abordagem tem-se que entender as diferenças normativas na regulamentação das telecomunicações, das redes e da internet no Brasil. De longe se vê a deficiência normativa no Brasil em relação ao tema. Se por um lado o Comitê Gestor da Internet fala da neutralidade das redes e a LGPD do tratamento dos dados, outro aspecto são os algoritmos enquanto relacionados a conceitos como a internet das coisas e outros vários aspectos.

Um outro aspecto é compreender que a internet, para falar apenas de um aspecto do problema a ser resolvido, é formada por várias camadas (***surface web, deep web e dark web***). O Brasil ainda se move a reboque dos demais países, como o Japão, que já discute a sociedade 5.0. A convergência digital traz com ela a nova era de tecnologias avançadas (sociedade 5.0).

O desconhecimento da área digital dificulta o enfrentamento normativo e leva os juristas a apoiar a elaboração de novas leis. Ocorre que o uso dos algoritmos possibilita o aumento da complexidade dos sistemas. Por outro lado, o interesse do mercado impede a criação de qualquer norma que venha barrar os seus interesses comerciais.

No tópico quatro apontam-se algumas falhas na tentativa de controle das redes, da internet e das mídias sociais digitais. O enfrentamento normativo é dificultado por diversos fatores, dentre eles a crescente evolução das tecnologias de comunicação e informação.

Do ponto de vista regulatório discussão importante é saber quem deva exercer a autoridade sobre ela, em que contexto e fundamentada em quais valores. A governança da internet oscila entre a regulação e autorregulação.

2 DIFERENÇAS NORMATIVAS NA REGULAÇÃO DAS TELECOMUNICAÇÕES, DAS REDES E DA INTERNET NO BRASIL

No ano de 1962, foi instituído no Brasil o Código Brasileiro de Telecomunicações- CBT , pela Lei n.º 4.117, de 27 de agosto. O seu artigo 4º definia os serviços de telecomunicações a difusão, envio ou recepção de símbolos, caracteres, sinais, escritos, imagens, sons ou elementos de qualquer natureza, através fio, rádio, eletricidade, meios óticos ou qualquer outro método eletromagnético[2]. Aqui não havia a distinção da radiodifusão. De igual modo ainda não se falava da internet, que viria a ser criada no ano de 1969. Entretanto, já contemplava serviço ponto-multiponto, denominado de serviço limitado.

A internet somente veio a ser criada no ano de 1969, nos Estados Unidos, na época da chamada "Guerra Fria". Chamada de Arpanet, era inicialmente utilizada com a função interligar laboratórios de pesquisa. Foi a época do primeiro e-mail, aí configurado como comunicação ponto a ponto.

Em 1985, a Embratel, sociedade de economia mista, criou o RENPAC – Rede Nacional de Comunicação de Dados por Comutação de Pacotes, rede comercial de transferência de pacotes (packet switched network), monocanal em operação duplex. Era regulada pela Portaria MC n.º 215, de 31 de agosto de 1987.

Em 1988, a internet chegou ao Brasil. O Marco Civil da Internet somente veio a ser definido em 2014, através da Lei n.º 12.965, de 23 de abril de 2014. Em 2021, já em um país pós *lockdown*, foi sancionada a Lei n.º 14.172, de 10 de junho, tratando da garantia de acesso à internet para a educação básica.

Através da Emenda Constitucional n.º 08[3], de 15 de agosto de 1995, foi alterado o inciso XI e a alínea "a" do inciso XII do artigo 21 da Constituição Federal. A alteração apartou as telecomunicações da radiodifusão, que antes eram juridicamente tratados juntos no Código Brasileiro de Telecomunicações. O inciso XI passou a prever a criação de um órgão regulador, que viria a ser a Anatel – Agência Nacional de Telecomunicações, criada pela Lei n.º 9.472/97 (Lei Geral de Telecomunicações - LGT)[4].

A LGT trouxe as definições de serviço de telecomunicações de serviço de valor adicionado (respectivamente artigos 60 e 61). O provimento de internet onde não haja o tratamento de dados configura-se como serviço de valor adicionado, visto por esta lei

[2] http://www.planalto.gov.br/ccivil_03/leis/l4117compilada.htm
[3]http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc08.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%208%2C%20DE,do%20%C2%A7%203%C2%BA%20do%20art.
[4] http://www.planalto.gov.br/ccivil_03/leis/l9472.htm

como atividade que acresce e dá suporte às telecomunicações, mas que com ele não se confunde. Desse modo o provedor qualifica-se como usuário do primeiro. Aliás, o mesmo artigo 61, em seu §2º, assegura o uso das redes de telecomunicações para a prestação de serviços de valor adicionado.

Em 2013 foi criado o Serviço de Comunicação Multimídia (SCM), através da Resolução nº 614 de 28/05/2013 / ANATEL - Agência Nacional de Telecomunicações (D.O.U. 31/05/2013).

O SCM é serviço de telecomunicações, prestado nacional e internacionalmente, em regime privado, que permite a oferta de capacidade de transmissão, emissão e recepção de dados multimídia, admitindo até mesmo o provimento de conexão à internet, por quaisquer meios, a seus clientes denominados de Assinantes correspondentes a determinada Área de Prestação de Serviço. Pode ser ponto a ponto e ponto-multiponto.

De logo já se vê a complexidade tratada pelo novo Direito Digital, ainda engatinhando enquanto específica área jurídica. Sua estimativa etária é de duas décadas apontando-se o seu nascedouro na Portaria Interministerial 147, de 31 de maio de 1995, editada pelos ministros da Comunicação e da Ciência e Tecnologia, que criou o Comitê Gestor Internet do Brasil (CGI)[5], foi o primeiro diploma legal desse ramo.

A Resolução CGI.br/RES/2012/003/P emitiu o posicionamento do Comitê Gestor Internet do Brasil em relação ao SOPA – Stop Online Piracy Act. A "Rede de Política & Jurisdição" foi fundada no âmbito da CGI no ano de 2012, movimentando atores de todo o mundo no sentido de entender a natureza transfronteiriça da internet. Nessa época ainda não se tinha a compreensão acerca da importância das questões jurisdicionais.

O Marco Civil da Internet (Lei n.º 12.965/2014), além de outras questões, fala da neutralidade de rede, a partir de seu artigo 9º, mas, já no artigo 2º reconhecia a importância da escala mundial da rede.

Antes de partir para a análise dos demais dispositivos normativos de importância para a elucidação do problema inicialmente proposto, necessária a diferenciação entre rede e internet: a rede incide em computadores fisicamente interligados e pode ser utilizado tanto como um computador pessoal como também para partilhar informações entre si; enquanto a internet é uma tecnologia que congrega as diminutas e amplas redes

[5] Criada pelo Decreto n.º 4.829, de 3 de setembro de 2003.[6] GUIMARÃES, Daiane Costa et al. Produção Científica Sobre A Sociedade 5.0. In: **10th International Symposium on Technological Innovation. 10th International Symposium on Technological Innovation. https://doi. org/10.7198/S2318-3403201900010918**. 2019, pág. 7.

entre si e edifica um circuito mais extenso. A terminologia “internet” é abreviada de “internetworking”, compondo um grupo de várias redes, como LAN, MAN e WAN, utilizando-se de softwares e hardwares apropriados, de funcionamento constante. Labora aplicando o conjunto de protocolos TCP / IP e o IP como protocolo de endereçamento.

A “World Wide Web” (www) transporta dados pertinentes a diversos campos, podendo referindo informações multifacetadas. É um conjunto de redes integradas, de alcance global. É disposta no desenho de “espinhas dorsais backbones”, que são arcabouços de rede dotados da possibilidade de manejar grandes volumes de elementos, formadas fundamentalmente por roteadores de tráfego integrados por circuitos de alta velocidade. Ligados às “espinhas dorsais”, estarão os provedores de acesso, os verdadeiros prestadores de serviços aos usuários finais. Se por um lado, os termos rede e internet aparentam estar no mesmo plano, isso não é verossímil, isso porque a rede pertence a algum grupo enquanto a Internet é aberta a todos os usuários.

A Lei n.º 13.853, de 8 de julho de 2019 veio alterar a Lei n.º 13.709, de 14 de agosto, passando esta última a ser conhecida como Lei Geral de Proteção de Dados (LGPD). Além de criar a Autoridade Nacional de Proteção de Dados (ANPD), traz mudanças significativas na fiscalização e aplicação de sanções. As empresas têm que adequar à LGPD, podendo sua conduta omissiva sofrer penalidades administrativas (art. 52) e Responsabilidade civil, moral e patrimonial (art. 42). Reconhece a aplicação subsidiária das normas correlatas (art. 64). Seu alcance abrange o âmbito público e privado, envolvendo as pessoas físicas e jurídicas. Não regula, entretanto o tratamento de dados de pessoas jurídicas e pessoais para fins não econômicos, jornalísticos, acadêmicos e de segurança pública (art. 4º). Importante a divisão trazida entre dados pessoais, sensíveis e anonimizados (art. 5º). O art. 13, § 4º refere à pseudonimização. O chamado encarregado pelo inciso VIII do art. 5º corresponde ao “Data Protection Officer” (**DPO**) e possui a atribuição de atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (art. 42, §2º).

De longe se vê a deficiência normativa no Brasil em relação ao controle das redes e da internet. Se por um lado o CGI fala da neutralidade das redes e a LGPD do tratamento dos dados., como ficam os algoritmos enquanto relacionados a conceitos como a internet das coisas (IoT), internet artificial, redes sociais e ao comportamento dos consumidores? Afinal, eles consistem em uma série de instruções, operações ou raciocínios com um escopo, algumas vezes voltados para a resolução de um problema.

Nem se fale da convergência digital das tecnologias (sociedade 4.0 e a evolução para a 5.0). O Serviço Móvel Pessoal ganhou destaque diante da forma compacta e do fácil manuseio do hardware e dos diversos softwares facilitados pelos aplicativos com finalidades diversas. O Serviço de Radiodifusão Sonora e de Sons e Imagens tem diuturnamente migrado aos chamados "celulares". Essa tem sido a prática de outros serviços como os antigos DTH e MMDS. O Serviço Limitado Privado, também migrou em seus vários aspectos para os aparelhos celulares. O que se tem assistido é a morte de vários serviços de telecomunicações e da radiodifusão como até então foram conhecidas. Essa é uma tendência mundial que no Brasil se tornará ainda mais efetiva com a entrada da tecnologia "5G".

No percurso das últimas duas décadas, a popularização da internet, a produção acadêmica acerca da liberdade de expressão, vista em seus limites e restrições progrediu em diferentes aspectos, mas, de maneira especial no Brasil, pode-se evidenciar pelo menos duas aparentes deficiências. Primeiro, resta evidenciada a escassez de pesquisa empírica, aprofundada, de testagem da aplicação pelo Poder Judiciário das sugestões doutrinárias consolidadas com fins à solução de conflitos entre a manifestação do pensamento, a honra e a imagem, sobretudo através do uso da avaliação e do princípio da proporcionalidade. Em um segundo viés, a grande maioria dos estudos presumem que a Justiça seria mais eficaz para a solução de tais conflitos, o que, mais uma vez, destaca a lacuna legislativa.

Parece posição mais acertada que a moderação da manifestação do pensamento na internet, a título de exemplo, deva ser efetivada através da autorregulação, no momento mais capaz de fazer frente aos problemas a serem solucionados, porque de processo normatizador mais rápido e de maior tangenciamento temporal. Afinal permite a relação dialógica entre plataformas de conteúdo e usuários aprovisionados de pretensões e capacidade de autogoverno e autonomia, no protagonismo determinante de quais devam ser as medidas concretas para inibi-las**.**

3 AS DIFERENTES CAMADAS DA INTERNET (*SURFACE WEB, DEEP WEB E DARK WEB*) E O ALCANCE NORMATIVO

Aos olhos do leigo, a grande maioria dos usuários, a web é a parte que se acessa para os conteúdos veiculados na internet. A "www" (*World Wide Web*). Não se esqueça que internet e web não são a mesma coisa. A *web* é a ferramenta de acesso à rede,

enquanto a internet representa a interconexão de computadores pelo mundo, onde se tem o e-mail, o FTP e inúmeras outras coisas. A *World Wide Web*, também é conhecida como *Surface Web*. Contudo ela é apenas a parte visível, um elemento superficial. Ainda se tem a *Deep Web* e a *Dark Web*. A partir da *Deep Web* os motores de busca como o famoso "Google" não interagem mais.

Se o que é visível, a *surface web* já traz em sua dialeticidade a dificuldade de normatização das condutas que nela atuam, de seus atores, as demais mais ainda. Interagindo com isso ainda se tem a capacidade e a velocidade do transporte de dados e suas influências e consequências. Quanto de dados pode suportar a fibra optica? A que velocidade os dados são transportados? Qual a segurança e confiabilidade da rede? Como se combate as condutas típicas, antijurídicas e culpadas segundo o ordenamento jurídico brasileiro? E a faixa de microondas enquanto ondas EM que aumentam o alcance dos dados transportados? Velocidade e alcance fazem da era digital um elemento dificultador do burocrático processo legislativo e do devido processo legal que tem a enfrentar o judiciário para tornar efetiva a tutela jurisdicional. A sociedade democrática exige para fazer valer os seus direitos fundamentais a demanda de certo tempo laboral e, essa demanda de tempo traz óbices inenarráveis à eficiência, eficácia e efetividade normativa.

Enquanto o Japão já estuda e publica sobre a sociedade 5.0 o Brasil sequer aparece no ranking dos principais países[6]. A convergência digital traz com ela a nova era de tecnologias avançadas (sociedade 5.0). Seria ela centrada na pessoa natural? A nova sociedade traz com ela o metaverso, o ciberespaço, tecnologias vestíveis, energia inteligente e muito mais.

A *Deep Web* é a camada que fica abaixo da Surface Web, menos visível por uma série de razões como segurança e privacidade. Apresenta-se como alternativa para a privacidade, porém permitindo por essa razão um ambiente propício para condutas ilícitas. A sua arquitetura funciona em versões como o TOR – The Onion Router. O navegador é o FIREFOX da Mozilla. Nesse ambiente se tem em relevo a segurança da informação e a proteção de informações sensíveis. Para isso se tornam importantes as criptografias, a criação de senhas fortes com alterações constantes, a análise de tráfego, o acurado zelo na prevenção e combate a programas suspeitos baixados ocultos e sem conhecimento do usuário.

---

[6] GUIMARÃES, Daiane Costa et al. Produção Científica Sobre A Sociedade 5.0. In: **10th International Symposium on Technological Innovation. 10th International Symposium on Technological Innovation. https://doi. org/10.7198/S2318-3403201900010918**. 2019, pág. 7.

Entram em cena os *hackers* e *crackers*. Os *hackers* como os indivíduos que modificam softwares e hardwares, criam e adaptam novos sistemas, com novas funcionalidades e aplicações. Os *crackers* se qualificam como os cibercriminosos e de igual modo dominam os códigos, a linguagem de máquina, os programas e as diferentes formas de acesso às redes. Como se vê, até aqui o desconhecimento impera e provoca uma confusão conceitual de implicações jurídicas relevantes.

Em um outro aspecto esses atores contribuem para a disseminação de "hoaxes" (boatos), um tipo de *spam*, onde a informação distorcida é enviada para o maior número possível de pessoas. Diferente do *spam* que tem fins comerciais ou golpista e dissemina de forma automatizada, sua propagação somente é satisfeita quando uma pessoa a espalha e os receptores, por sua vez, de igual modo repetem o ato. Pode também veicular "malwares".

Similar aos "hoaxes", mas guardando dessemelhanças em relação a eles, atualmente se fala nas "fake News" ou notícias falsas. O aumento do número de usuários da internet, grande parte devido aos smartphones, contribuem para o crescimento dos noticiosos inverídicos. Muitos passam o dia em mídias sociais como o Instagram e, grande parte acaba divulgando notícias ali veiculadas sem checar a fonte ou a veracidade das informações.

O compartilhamento de informações fraudulentas tem graves consequências. Isso levou o Supremo Tribunal Federal a instituir o Programa de Combate à Desinformação (PCD) no âmbito da instituição, através da Resolução n.º 742, de 27 de agosto de 2021.

Os crimes conexos com anonimato na internet servem de propaganda para aumentar o interesse pela *Deep Web* e *Dark Web*. A *Dark Web* faz parte da *Deep Web*, no entanto, é parte bem pequena, e voltada somente à prática de crimes. Pode ser acessada por intermédio de nós descentralizados e anônimos em uma série de redes incluindo TOR (abreviação de The Onion Router) ou I2P (Invisible Internet Project), rede totalmente privada e criptografada. Na *surface web* é oferecido acesso a esta última bastando baixar o seu software.

A *Dark Web*, possui teor que foi oculto propositalmente. Pode ser acessada para fins legítimos, , para ocultar criminosos ou atividades maliciosas. Tome-se a título de exemplo a "Rota da Seda", que era uma rede global online de serviços ilícitos e contrabando, especialmente drogas. Traficantes de substâncias ilegais foram localizadas em mais de dez países do mundo, forneceu a mais de cem mil compradores. Foi

considerado que a “Rota da Seda” gerou cerca de US $ 1,2 bilhão nas vendas em três anos, antes do desmonte pelos agentes federais.

O uso da *Dark Web*, para fins ilícitos levou o legislativo americano a questionar se teria suficientes ferramentas para combater as atividades ilícitas em atuação nesse submundo. Os usuários não podem acessá-la sem um software especial. Os editores desses sites estão ocultos. Os usuários do “TOR” se conectam a sites através de uma série de túneis virtuais ao invés de fazer uma conexão direta, permitindo assim que as organizações e indivíduos compartilhem informações em redes públicas sem comprometer sua privacidade. Os usuários encaminham seu tráfego da web através de computadores de outros usuários, de modo que o tráfego não possa ser rastreado para identificação do usuário original. O TOR essencialmente estabelece camadas, como se fosse as camadas de uma cebola, e direciona o tráfego através dessas camadas para ocultar as identidades dos usuários. Para ir de uma camada para outra, o TOR estabeleceu um “retransmite” em computadores de todo o mundo através dos quais as informações são conduzidas. A informação é criptografada entre as retransmissões, e todo o tráfego do TOR passa por pelo menos três retransmissões antes de chegar ao seu destino. Ao utilizar o TOR, os endereços IP dos usuários permanecem ocultos.

Os criminosos antes comuns, agora do mundo digital, os cibercriminosos, dependem cada vez mais da Internet e de tecnologias avançadas para exercerem suas operações ilícitas. Vários crimes são impulsionados pela internet, como furto de identidade e de propriedade intelectual, clonagem de cartões, negociações e tráfico de entorpecentes, pedofilia, tráfico humano, para citar apenas alguns. Os crimes utilizando as altas tecnologias cada vez mais se sofisticam e especializam-se. A legislação é insuficiente para contê-los.

A *Dark Web* também pode fornecer uma plataforma para os criminosos venderem bens ilegais ou roubados. No aspecto das violações de dados, por exemplo, pode ser o veículo para aquisição de *malware* usado em violações de dados em grande escala para capturar crédito não criptografado e as informações de cartões de débito.

Os cibercriminosos podem vitimizar indivíduos e instituições, e podem fazê-lo sem limitações de fronteiras. Isso se torna um desafio permanente para a aplicação da lei uma vez que fica difícil precisar o local do crime.– e explorou-os. Fronteiras físicas-cibernéticas. As fronteiras relativamente claras no mundo físico nem sempre são assim no reino virtual. O ciberespaço ultrapassa as fronteiras físicas, as fronteiras dentro do ciberespaço – jurisdicional e tecnológica - ainda existem. Alguns endereços da web são

específicos de cada país e a administração desses sites é controlada por nações específicas.

4 OS ALGORITMOS E O ENFRENTAMENTO NORMATIVO

Os algoritmos podem ser definidos como uma sequência de regras que, uma vez aplicadas a determinado numero de dados, possibilita engendrar classes semelhantes de problemas. São, na informática e telemática, o conjunto de normas e procedimentos lógicos impecavelmente marcantes que induzem à solução de problema em um número de fases. Os sistemas algorítmicos encontram-se presentes em vários lugares, mas assumiram maior grau de importância com a convergência digital. Com eles também evoluíram a *artificial intelligence, machine learning, neural networks* e *internet of things*.

O desconhecimento da área digital leva os juristas a apoiar a elaboração de novas leis. Ocorre que os algoritmos permitem que os sistemas cada vez mais aumentem em complexidade. Nem se fale que o interesse do mercado impede a criação de qualquer norma que venha barrar os seus interesses. Processos algorítmicos vem sendo empregados para influenciar condutas. O Processamento algorítmico não deve ser a única base para uma decisão que produza efeitos jurídicos ou possa impactar os direitos de qualquer indivíduo.

Alguns defendem alocar estes tipos de códigos e algoritmos intricados no domínio público para que todos possam auditá-los. Entretanto, pouca utilidade se tem na aferição de responsabilidades pela má utilização da tecnologia. Basta dizer que vulnerabilidades em determinados algoritmos, de código aberto, de ampla divulgação pública e largamente utilizados e com a devida auditoria, levaram muito tempo para sua identificação. Daí os defensores de que a padronização da transparência algorítmica não pode ser definida em norma, uma vez que as especificidades tecnológicas possuem larga variação espectral.

A regulação parece ser utópica. A dinamicidade das modificações impõe vários óbices à regulamentação. Em outro aspecto, não se pode esquecer que os algoritmos, não são imunes ao viés político, aos interesses de mercados e ao uso de alcance político, militar, e do serviço de inteligência. A auditoria na inteligência artificial envolve várias áreas não tecnológicas, dentre elas o Direito e a Ética.

Quando qualquer um, hoje em dia, adquire pela primeira vez um aparelho móvel pessoal, um smartphone, em primeiro lugar, a sua opção pela marca vai distinguir que sistema operacional irá utilizar. Mas independente disso, ao acessar a rede e ao realizar o

download de aplicativos, permitirá à rede, ininterruptamente, traçar e retraçar o seu perfil nos mais diferentes níveis, a ponto de identificar seus gostos, seus problemas de saúde, sua opção sexual, seu perfil socioeconômico, os lugares por onde anda e muito mais. A título de exemplo o *tripwire* revela-se como uma estratégia de venda e posterior fidelização do cliente. Oferece-se um *low ticket*, uma isca digital, onde se coletam e-mails, número de telefone, entre outros dados.

Ao acessar a internet ou o Instagram e Facebook, deixam-se as chamadas "pegadas digitais", criando identidades nelas alicerçadas e permitindo a algoritmos bem estruturados acompanharem os acessos e formularem perfis os mais diversos. Na era do progresso digital e da inovação tecnológica também se aprimoram os bens e serviços, deixando ocultos a manipulação, a discriminação e a sujeição a decisões de inteligências artificiais que não são alcançadas pela Lei Geral de Proteção de Dados porque, simplesmente não vem a público e são realizadas *interna corporis*.

Mesmo que se considere o fato de que se os algoritmos inteligentes não estiverem dotados dos predicados necessários para o abastecimento de uma explicação – e enquanto não permanecerem –, a sua utilização é ilícita, o rastreamento, controle e punição são de difícil efetivação. A opacidade dos algoritmos seria um dos maiores estorvos à sagração de regime legal concernente às disposições automáticas capaz de afiançar uma tutela eficaz da personalidade humana e que a cristalinidade seria o maior instrumento de combate. Contudo a transparência não é suficiente para alcançar tal exigência. A tutela conferida pela LGPD é claramente insuficiente.

O expediente de se utilizarem conceitos indeterminados é imperativo para que o expediente normativo não se deixe suplantar pela célere evolução tecnológica, entretanto não beneficia a certeza e segurança jurídicas. As assimetrias de informação que distinguem a relação posta entre o responsável pelo tratamento e o titular dos dados e as possíveis implicações lesivas do tratamento relevam que as imprecisões sejam invalidadas em benefício do titular dos dados, desde que encontrem um mínimo de correspondência com a letra da lei. O aspecto jurídico das decisões automatizadas é do mesmo modo carregado de empecilhos interpretativos, sobremaneira no que pertine ao direito de não sujeição às decisões automatizadas.

5 FALHAS NA TENTATIVA DE CONTROLE DAS REDES, DA INTERNET E DAS MÍDIAS SOCIAIS DIGITAIS

O uso da internet no Brasil corresponde hoje a aproximados 81% da população, alcançando 152 milhões de brasileiros, com crescimento significativo entre o que chamam de classes "D" e "E", o que fica em torno de 67%[7].

De olho nessa estatística em números crescentes, todos aqueles que de algum modo podem se beneficiar, direta ou indiretamente, passam a visar a manipulação das tecnologias de comunicação e informação. Em um aspecto, desde a emergência da *web* em idos de 1991, a democratização da rede foi acompanhada pela privatização de parte de sua infraestrutura, bem como pelo surgimento de instituições para garantir o seu funcionamento. Os estados têm buscado um maior intervencionismo, porém a autorregulação ainda prevalece. Foi no final de 1990 que veio à baila a questão da governança da internet. Ali já se buscava a criação de uma forma de autoridade que permitisse a coordenação e a regulamentação. A governança coordenava os nomes dos domínios e endereços. O DNS (*Domain Name System*) está diretamente relacionado com os desafios da regulamentação, para entender a que se presta um site. Mas, como já se demonstrou, isso, na *surface web*. O DNS pode ser descontinuado ou controlado. Não se pode deixar de lado a gestão dos recursos críticos da rede, a proteção da propriedade intelectual, a segurança cibernética e a regulamentação dos conteúdos.

No início do ano 2000 a governança da internet juntava-se à estratégia da neutralidade das redes. Seria uma extensão da noção norte-americana do *common carrier*. A neutralidade das redes a partir daí, apresentou-se como um embasamento normativo para a governança da internet. Um sentido ambíguo, onde se tem a intervenção em nome da livre circulação de informação, com igualdade de processamento dos fluxos e obstaculizando a priorização de determinados conteúdos e serviços.

Não se pode esquecer da jurisdição, quando o problema, em atendimento ao Direito Individual do inciso XXXV do art. 5º da CF evocar a tutela jurisdicional do estado-juiz. Aqui se ilustra uma situação para se demonstrar a complexidade que mesmo o simples controle e regulamentação do DNS pode trazer. Suponha que "A" entregou o seu computador para a empresa "X" consertar, mas, esqueceu em um de seus arquivos, na pasta "documentos" 477 fotos íntimas. O empregado "C" resolveu divulgá-las no site "caiu na net". Ao descobrir suas fotos no site "A" ingressa com ação judicial para a devida retirada de circulação, entretanto, ao obter a ordem liminar, as fotos já foram replicadas

[7] "TIC Domicílios 2020", elaborada pelo Cetic.br (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação), apoiado pela Unesco, e pelo Cgi.br (Comitê Gestor da Internet no Brasil)

em sites estrangeiros que outros sites brasileiros têm acesso através de “links” em suas páginas. Veja-se que o controle enfrenta diversos contratempos, no próprio sistema jurídico nacional e internacional.

A cada filtro que se coloque nas mídias sociais para impedir os *hoaxes* e as *fakes news*, dada a dinamicidade e a complexidade das redes, da internet, dos algoritmos e de tudo mais envolvido com as tecnologias de comunicação e informação e a convergência digital, não se consegue, efetivamente coibir de forma contundente que notícias e informações não condizentes com a verdade sejam veiculadas. Uma notícia pode ser excluída e repostada em outro lugar por uma outra pessoa em um outro lugar, a uma velocidade muito maior que o alcance da *longa manus* da vetusta justiça.

Nem se fale que a arquitetura do código de programação, exibida para os usuários através da interface do ambiente virtual, é volta e meia descurada pela presteza jurídica, mas se manifesta como um elemento basilar na cadeia causal da dispersão de notícias falsas. As redes sociais realizam controle editorial automático de conteúdos produzidos pelos usuários, com resultados individualizados, mas obedecendo a um parâmetro de "importância" determinado. O que de fato é estimado como relevante pelo algoritmo aparentemente trata-se de conteúdos que promovem maior engajamento do usuário com a rede social, objetivando uma maior quantidade de dados pessoais comercializáveis pela rede, beneficiando a dispersão de notícias pérfidas.

Inegavelmente o direito, na maioria das vezes, vem em contraponto aos fatos, o que nas dinâmicas disruptivas é ainda mais percebível, uma vez que tais modelagens progridem na vida social em rapidez inconciliável com a produção normativa.

6 CONSIDERAÇÕES FINAIS

A internet na proporção em que evoluiu em complexidade e se tornou cada vez mais relevante quanto ao fator econômico e político. O incremento mercadológico com o crescimento do interesse comercial, aliado ao aumento das operações mercantis, da individualização do controle sobre as mídias de informação, contribuíram para que fosse revista a liberdade irrestrita, reafirmando a opção reguladora na proporção em que se apresentavam judicialmente os casos de ciberempresas e de cibercrimes.

O aumento da percepção de que as redes não eram um espaço à parte e o surgimento de microempresas no modelo *start up* passou a encontrar obstáculos. A economia digital permitiu um setor mais concentrado. A judicialização no sentido de

territorializar os acontecimentos no âmbito da internet, a luta contra as violações de direitos autorais via *peer to peer* de arquivos musicais e o aumento da cibercriminalidade com a disseminação de pornografia e de negociações de tráfico humano e de drogas no ambiente abaixo da *surface web*, também cresceu. Tangenciando essas questões cresceu em demasia a preocupação com a segurança nacional com a implantação de protocolos mais avançados de vigilância.

A internet, dentro do que a maioria dos usuários enxergam, conduz as problemáticas sociais, econômicas, políticas e geopolíticas, na mesma medida em que conduz os *hoaxes* e as *fake news*. Do ponto de vista regulatório discussão importante é saber quem deva exercer a autoridade sobre ela, em que contexto e fundamentada em quais valores. A governança da internet oscila entre a regulação e autorregulação. Daí discussão importante é a neutralidade das redes, no contexto do uso indiscriminado da internet banda larga. Contrapõem-se as posições do ciberlibertarianismo com ciberanarquismo. A regulamentação deve levar em conta as complexas interações assim como a diversidade dos atores, dos desafios tecnológicos, e de diversos outros aspectos. As principais fontes de regulamentação na internet, articuladas com as regras do direito, reforçam o reconhecimento das escolhas de arquiteturas de software e hardware.

Se por um lado os protocolos de TCP/IP da internet permitam em tesse impedir o controle da circulação da informação ante a constatação do conhecimento dos conteúdos, da identificação dos remetentes e dos destinatários dos dados veiculados; em outro aspecto, tem-se a dificultação pela destinação dos dados coletados pelas inteligências artificiais, no uso indiscriminado dos algoritmos, além de *tripwires* e de *honeypots*, para citar apenas alguns aspectos.

O mundo tecnológico, de uma dialeticidade multifacetada, na evolução para a Sociedade 5.0, traz o desafio da necessidade de proteção da sociedade e das organizações. A autorregulação tem se apresentado como a melhor contrapartida para a resposta mais efetiva às intempéries apresentadas.

No caso das *fake news*, por exemplo, o que não se pode é, em nome da defesa das liberdades fundamentais, implementar-se a censura, em detrimento da liberdade de expressão. Isso representaria um retrocesso sob a ótica do constitucionalismo.

O Ciberespaço, por si, não pode cumprir as promessas de liberdade. É possível modelar uma arquitetura impulsionada pelo Estado e pelo mercado no sentido de uma regulamentação eficaz. Há de se adotar cautela ante a possibilidade de ameaças às liberdades. A Constituição identifica os valores substanciais que devem ser garantidos de

modo a permitir escolhas de modo estrutural inspiradas no sistema de "*checks and balances*".

REFERÊNCIAS

ÁLVAREZ-CIENFUEGOS SUÁREZ, José María. 1999. **La defensa de la intimidad de los ciudadanos y la tecnología informática**. Pamplona: Aranzadi. ASIA-PACIFIC ECONOMIC COOPERATION (APEC). 2004. APEC privacy framework, adoptado en la 16a Reunión Ministerial de APEC, 17 y 18 de noviembre de 2004, Santiago de Chile.

AFONSO, Carlos A. Internet no Brasil–alguns dos desafios a enfrentar. **Informática Pública**, v. 4, n. 2, p. 169-184, 2002.

ARAÚJO, Marcelo Barreto de. Comércio eletrônico; Marco Civil da Internet; **Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviço e Turismo, 2017.

BALKIN, Jack M. **O futuro da liberdade de expressão na era digital**. Liberdade de expressão no Século XXI. SAMPAIO, José Adércio. Belo Horizonte: Del Rey, 2016.

BARLOW, John Perry. 1996. A Declaration of the Independence of Cyberspace, 8 de febrero. Davos, Switzerland. Disponível em: . Último acesso em: 16 Mar. 2013.

BRASIL. **Lei n.º 4.117, de 27 de agosto de 1962**. Institui o Código Brasileiro de Telecomunicações.

_____. Emenda Constitucional n.º 8, de 15 de agosto de 1995. Altera o inciso XI e a alínea "a" do inciso XII do art. 21 da Constituição Federal.

_____. **Lei n.º 9.472, de 16 de julho de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.

_____. **Decreto n.º 4.829, de 3 de setembro de 2003**. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências.

_____. **Resolução nº 614 de 28/05/2013** / ANATEL - Agência Nacional de Telecomunicações (D.O.U. 31/05/2013). Aprova o Regulamento do Serviço de Comunicação Multimídia e altera os Anexos I e III do Regulamento de Cobrança de Preço Público pelo Direito de Exploração de Serviços de Telecomunicações e pelo Direito de Exploração de Satélite.

_____. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

_____. **Lei n.º 13.709, de 14 de agosto**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019)

_____. **Lei n.º 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

BROWN, Ian. Autorregulação na internet e os direitos fundamentais. **Liberdade de expressão no Século XXI**. SAMPAIO, José Adércio. Belo Horizonte: Del Rey, 2016.

COUTO, Idelvania Ferreira et al. Governabilidade na rede: liberdade e controle do espaço virtual. **REVISTA JURÍDICA DA FAMINAS**, v. 7, n. 1-2, 2015.

DA SILVEIRA, Sergio Amadeu. Liberdade, diversidade e controle na internet. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, v. 4, n. 4, 2010.

DE ALMEIDA, Leonardo Pinto. AS ALIANÇAS ENTRE AS ARQUITETURAS DO CONTROLE, AUTORIA, COMÉRCIO E MEIO DIGITAL. **Informação & Sociedade**, v. 18, n. 3, 2008.

EHLE, Géssica Adriana; GOULART, Gil Monteiro. A DEMOCRACIA NA CONTEMPORANEIDADE: A PARTICIPAÇÃO CIDADÃ E AS NOVAS FORMAS DE CONTROLE SOCIAL DIANTE DAS NOVAS TECNOLOGIAS. **Revista Palotina de Estudos Jurídicos e Sociais**, v. 2, n. 1, 2016.

EMPOLI, Giuliano da. Os engenheiros do caos. Como as fake News, as teorias da conspiração e os algoritmos estão sendo utilizadas para disseminar ódio, medo e influenciar eleições.

FREDES, Andrei Ferreira. 16. LIBERDADE DE EXPRESSÃO E CONFIGURAÇÃO DO AMBIENTE VIRTUAL: O CONTROLE DO FLUXO DE INFORMAÇÃO E EXPRESSÃO NA INTERNET. **Direito, Ambiente e Tecnologia: estudos em homenagem ao professor Carlos Alberto Molinaro**, p. 401.

GUIMARÃES, Daiane Costa et al. Produção Científica Sobre A Sociedade 5.0. In: **10th International Symposium on Technological Innovation. 10th International Symposium on Technological Innovation. https://doi. org/10.7198/S2318-3403201900010918**. 2019.

HOFFMANN-RIEM, Wolfgang. Controle do comportamento por meio de algoritmos: um desafio para o Direito. **Direito Público**, v. 16, 2019.

HUPFFER, Haide Maria; PETRY, Gabriel Cemin. (Des) Controle digital de comportamento e a proteção ao livre desenvolvimento da personalidade: Digital (un) control of behavior and the protection of free development of personality. **International Journal of Digital Law**, v. 2, n. 1, p. 111-132, 2021.

KAISER, Brittany. **Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque**. HARLEQUIN, 2020.

LOVELUCK, Benjamin. **Redes, liberdades e controle: uma genealogia política da internet** . Editora Vozes Limitada, 2018.

LYONS, John; MOTA, Octanny Silveira da; HEGENBERG, Leônidas. As ideias de Chomsky. In: **As ideias de Chomsky** . 1970. p. 121-121.

MACHADO, Vinicius Rocha Pinheiro; DIAS, Jefferson Aparecido; FERRER, Walkiria Martinez Heinrich. Biopolítica e novas tecnologias: o discurso do ódio na internet como mecanismo de controle social. **Revista de Informação Legislativa**, v. 55, n. 220, p. 29-51, 2018.

MADALENA, Juliano. Regulação das fronteiras da internet: um primeiro passo para uma Teoria Geral do Direito Digital. **Revista dos Tribunais**, v. 974, p. 81-110, 2016.

MAGRO, Americo Ribeiro. A INVIOLABILIDADE DOS DADOS PESSOAIS E O CONTROLE JUDICIAL DA PROVA ELETRÔNICA ILÍCITA. **Revista Brasileira de Direitos e Garantias Fundamentais**, v. 4, n. 2, p. 61-82, 2018.

MOTA, Ronny Cesar Camilo. **Direito de Mídia: instrumento de liberdade ou de controle?**. Editora Dialética, 2021.

NUNZIATO, Dawn C. 2009. **Virtual freedom**: net neutrality and free speech in the Internet age. Standford, CA: Stanford Law Books.

PATTERSON, James T. 2010. **Freedom is not enough**: the Moynihan report and America's struggle over black family life: from LBJ to Obama. New York: Basic Books.

PEREIRA, Ana Julia Zuquim Ferreira; SEVERO, Laura Lima; LANGOSKI, Deisemara Turatti. LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL: BREVE ANÁLISE SOBRE O DIREITO À PRIVACIDADE. **Anais do Salão Internacional de Ensino, Pesquisa e Extensão**, v. 13, n. 3, 2021.

PIMENTA, Ricardo M. Big data e controle da informação na era digital. **Tendências da Pesquisa Brasileira em Ciência da Informação**, v. 6, n. 2, 2013.

RODRIGUES, Horácio Wanderlei; BECHARA, Gabriela Natacha; GRUBBA, Leilane Serratine. Era Digital e Controle da Informação. **Revista Em Tempo**, v. 20, n. 1, 2020.

SILVEIRA, Marilda de Paula. As novas tecnologias no processo eleitoral: existe um dever estatal de combate à desinformação nas eleições. **Fake news e regulação. São Paulo: Thomson Reuters Brasil**, p. 191-216, 2018.

SILVA, Tarcizio. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. **COMUNIDADES, ALGORITMOS E ATIVISMOS DIGITAIS**, p. 121, 2019.

STF. Resolução n.º 742, de 27 de agosto de 2021. Institui o Programa de Combate à Desinformação no âmbito do Supremo Tribunal Federal.

TAVARES, André Ramos; BITENCOURT, Caroline Muller. Diálogo entre o Direito e a Engenharia de Software para um novo paradigma de transparência: controle social digital. **Revista Eurolatinoamericana de Derecho Administrativo**, v. 8, n. 1, p. 9-34, 2021.