Microssistema jurídico do ambiente digital

2ª Edição – revista e ampliada (outubro – 2023)

Caio Sperandéo de Macedo

Emerson Penha Malheiro

Fabio Romeu Canton Filho

Greice Patricia Fuller

Irineu Francisco Barreto Junior

Jorge Shiguemitsu Fujita

Jose Marcelo Menezes Vigliar

Nivaldo Sebastião Vícola

Samyra Haydee Dal Farra Naspolini

Tiago Cappi Janini

Dados Internacionais de Catalogação na Publicação (CIP)(Câmara Brasileira do Livro, SP, Brasil)

Microssistema jurídico do ambiente digital [livro eletrônico]. -- 2. ed. rev. e ampl. -- São Paulo, SP : Ed. dos Autores, 2023.
PDF

Vários autores.
Bibliografia.
ISBN 978-65-00-84213-5

1. Direito digital 2. Proteção de dados - Direito - Brasil 3. Sociedade da informação - Aspectos jurídicos.

23-178083 CDU-34:004

Índices para catálogo sistemático:

1. Direito digital 34:004

Tábata Alves da Silva - Bibliotecária - CRB-8/9253

I - PROPOSTA DOUTRINÁRIA

1. Apresentação.

A construção doutrinária que estamos apresentando e que poderá ser aperfeiçoada pela comunidade jurídica, trata do que, de forma inédita, estamos denominando de *microssistema jurídico do ambiente digital*, que versa sobre a proteção de dados pessoais e os limites da aplicação das novas tecnologias do ambiente digital como é o caso da *inteligência artificial*.

Tal concepção decorre da troca de conhecimentos e de reflexão coletiva dos docentes do Mestrado em Direito da Sociedade da Informação do Centro Universitário das Faculdades Metropolitanas Unidas, que ocorreu, principalmente, a partir das atividades (palestras com especialistas, entrevistas, apresentação de trabalhos científicos, gravação de podcasts etc.) desenvolvidas no âmbito do Congresso Acadêmico FMU/FIAM-FAAM *"Inteligência Artificial: Realidade e Projeções"* (https://www.even3.com.br/congresso-fmu-fiam-faam/) realizado entre os dias 15 e 19 de maio de 2023, nos *campi* do Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo, Brasil, com mais de (18) dezoito mil inscritos.

2. Preâmbulo.

Para a compreensão da importância da proteção de dados, podemos contextualizar o momento histórico em que vivemos denominado por muitos autores de Sociedade da Informação. Conforme Roberto Senise Lisboa (2006, p. 115), trata-se do período histórico em que a informação prevalece sobre os meios de produção e distribuição dos bens.

Assim sendo, a Sociedade da Informação faz surgir "complexas redes profissionais e tecnológicas voltadas à produção e ao uso da informação, que alcançam ainda sua distribuição através do mercado, bem como as formas de utilização desse bem para gerar conhecimento e riqueza". (BARRETO JR, 2007, p. 2)

Para Takahashi a Sociedade da Informação é um fenômeno global que traz uma profunda mudança nas atividades sociais e econômicas, havendo quem a considere "um novo paradigma técnico-econômico." (TAKAHASHI, 2000, p. 5) Neste contexto a tecnologia e a comunicação se tornaram aspectos centrais do desenvolvimento social, fazendo surgir novas violações de direitos nas relações públicas e privadas.

Assim, se torna cada vez mais imperiosa a proteção dos Direitos Humanos Fundamentais frente às possibilidades de violação trazidas pelas novas tecnologias, podendo-se falar na convergência de sujeitos como o poder público, o sujeito particular, as empresas e a coletividade como ao mesmo tempo sujeitos desses direitos e responsáveis pela sua proteção e concretização.

3. O Microssistema jurídico

O conceito de microssistema evoluiu e não representa apenas uma alternativa à codificação que, aparentemente, constitui um modelo tanto mais rígido (para ser constituído), quanto mais complexo (em relação ao seu conteúdo) e mais perene (quando se cogita de sua modificação). Efetivamente, existe uma maior resistência para a substituição e ou modificação de um código. A modificação das leis esparsas, constitui uma atividade menos complexa e não gera tanta resistência.

Os microssistemas jurídicos justificavam suas concepções sob o fundamento de que uma única lei poderia tratar de aspectos materiais e processuais sobre determinado tema. Assim ocorreu com dois contundentes exemplos, um na área da proteção do consumidor, outro na área de proteção da criança e do adolescente (respectivamente, a Lei nº 8.078, de 11 de setembro de 1990 e a Lei nº 8.069, de 13 de julho de 1990)

Ainda que sejam denominados de "códigos" ou "estatutos" foram decretados e sancionados sem que grandes alterações nos Códigos então vigentes fossem necessárias.

Veicularam tipos penais específicos, versaram sobre responsabilidade civil, modificaram a distribuição dos ônus de provar, fixaram normas de competência para o exercício da jurisdição, criaram um sistema de aferição da legitimidade ativa para demandas coletivas, trataram da extensão dos efeitos subjetivos da coisa julgada material, entre outras providências.

Nos principais exemplos de microssistemas vigentes temos leis federais que, editadas conforme as normas previstas na Constituição Federal, constituem leis que derrogam, em muitos aspectos, a disciplina legal prevista nos códigos para aqueles mesmos temas.

Essa é uma virtude inquestionável dos microssistemas, que têm a capacidade de criar relações entre diplomas legais que se complementam e, ainda, proporcionar a aplicação de dispositivos dos códigos em caráter complementar, sempre que não houver disciplina específica em sentido contrário ou contrariar normas e princípios que tutelam, apresentando a notável propriedade de contribuir com a coesão social ao desempenhar um papel importante na promoção da justiça e na resolução de conflitos, propiciando maior estabilidade e segurança jurídica para as relações interpessoais, além de possuírem conteúdos específicos e criarem linguagem específica.

Os microssistemas jurídicos, portanto, traduzem essencialmente a ruptura com a estrutura dos códigos (especialmente, no que se refere à subordinação com algum ramo específico da dogmática jurídica), vindo a possuir características próprias de interdisciplinaridade (por vezes, multidisciplinaridade), principiologia e vinculação direta à logica constitucional, caracterizando-se por modelos de unidade e ordenação, mas com relações a outras normas do ordenamento jurídico.

Analisemos um paradigma extremamente eficaz, antes de considerarmos o microssistema da proteção dos dados e utilização da inteligência artificial e a necessidade de sua integração.

4. O paradigma do microssistema da tutela jurisdicional coletiva.

Algumas garantias constitucionais do cidadão ditaram a concepção do microssistema da tutela jurisdicional coletiva, destacando-se a inafastabilidade do controle jurisdicional; contraditório; eficácia dos limites subjetivos da coisa julgada material (todos expressamente previstos no art. 5º, incisos XXXV, LV e XXXVI).

Todas essas garantias integram a cláusula do devido processo legal, prevista no inciso LIV do mesmo art. 5º.

O Código de Processo Civil então vigente – e o atualmente vigente também (*vide* o art. 17 da Lei n° 13.105 de 16 de março de 2015) – são diplomas de modelo individualista, baseados na subjetividade dos direitos, exigindo a avaliação prévia da condição da ação denominada "legitimidade de parte" para o exercício do direito de ação.

O máximo que esses diploma garantem é a formação de litisconsórcio (pluralidade de partes). Os litisconsórcios não dispensam a análise prévia e individual da legitimidade de cada um dos litisconsortes.

A legitimidade é a garantia da possibilidade de participação em contraditório e, assim, da posterior imposição do julgado às partes, considerando que a participação lhes foi franqueada.

Ficavam à margem da proteção jurisdicional os direitos e interesses transindividuais, principalmente aqueles que são indivisíveis. Não há como realizar a defesa dos interesses de um ou alguns dos interessados sem que todos os demais sejam atingidos pelo resultado prático do processo.

Como impor o julgado a quem não participou do contraditório instituído perante o juízo competente?

Os juristas brasileiros verificaram que havia a possibilidade de adoção do sistema de representação adequada de todos os interessados, mediante a verificação de critérios relacionados às funções que determinadas instituições desempenhavam ou poderiam desempenhar.

Tais instituições representariam a coletividade em juízo. Como autoras, teriam o ônus de produzir as provas dos fatos constitutivos do direito afirmado. Para que se desincumbissem desse ônus, a extensão subjetiva da coisa julgada material foi relativizada.

A improcedência dos pedidos deduzidos só alcançaria a todos caso a prova produzida fosse suficiente, situação que deveria ficar absolutamente clara na sentença que julgasse tais pedidos.

Um exemplo pode ilustrar todos esses pontos. Imagine-se a poluição do meio ambiente. Tal interesse é indiscutivelmente indivisível. Impossível imaginar-se que a poluição atinja a uns indivíduos e não atinja a toda a humanidade, ainda que possamos circunscrever aqueles que se prejudicariam de forma mais expressiva, dada a proximidade com a localidade atingida.

A propositura de uma ação, mediante a utilização dos mecanismos de aferição da legitimidade previstos no Código de Processo Civil era impossível.

Naturalmente, ao tutelar o direito de uma pessoa, o direito de todas as demais estaria implicado.

Sujeitar-se ao julgado sem a participação no contraditório, sobretudo na produção da prova (no caso, de quem poluiu, como poluiu, as consequências da poluição etc.) seria subverter as garantias anteriormente mencionadas.

Duas alterações foram realizadas, conforme mencionado. Um representante adequado desse conflito como, por exemplo, uma associação civil cujos objetivos estatutários sejam relacionados à proteção do meio ambiente, poderia representar, em juízo, a todos os interessados, ajuizando a ação. Posteriormente, a extensão dos efeitos subjetivos da coisa julgada material (a todos) caso os pedidos fossem julgados improcedentes ficaria na condição de a prova produzida ser suficiente ao convencimento do juízo.

Em um período anterior e bem próximo à promulgação da Constituição Federal de 1988, foi editada a denominada Lei da Ação Civil Pública (Lei nº 7.437 de 24 de julho de 1985) que, acrescente-se, foi recepcionada pela nova ordem constitucional.

Foi um marco legislativo importantíssimo, pois possibilitou a defesa em juízo dos interesses difusos e coletivos.

Entre 1985 e nos anos 1990 inúmeros artigos e livros foram produzidos. Dissertações de mestrado, teses de doutoramento, livre-docência e titularidade passaram a se ocupar do tema.

Aproximadamente cinco anos depois, foi promulgado o Código de Defesa do Consumidor, mencionado no início das presentes considerações.

Referido código – isoladamente considerado – constituiu um verdadeiro microssistema. Contudo, a lei de 1990 fez mais, pois derrogou a Lei da Ação Civil pública, criando uma eficácia de reciprocidade entre esses dois diplomas que, na prática, permitem identificar toda a disciplina processual para a tutela dos interesses transindividuais.

Vale mencionar que identificou os elementos constitutivos dos interesses difusos e coletivos, destacando-lhes a indivisibilidade como característica essencial; disciplinou a tutela aos interesses individuais homogêneos que, a despeito de individuais, podem ser tutelados de forma coletiva, considerando que têm a mesma

origem; cuidou da extensão dos limites subjetivos da coisa julgada para cada um dos três grupos de interesses transindividuais e uniu-se com menção recíproca de eficácia com a Lei da Ação Civil Pública.

Referidas leis formaram um microssistema que permitiu que a inafastabilidade do controle jurisdicional se tornasse uma realidade, possibilitando que os interesses transindividuais tivessem acesso à justiça.

5. Fundamentos teórico e legal formadores do microssistema de proteção de dados.

Verificamos, conforme referido anteriormente, que no âmbito digital, há um cenário que reclama pela identificação de um microssistema para a proteção de dados e utilização da inteligência artificial.

Sobretudo depois da Emenda Constitucional 115, de 10 de fevereiro de 2022, que acresceu o inciso LXXIX ao art. 5º da Constituição Federal de 1988, assegurando que, nos termos da lei, fica garantida a proteção de dados pessoais, inclusive nos meios digitais.

Referida garantia constitucional, por sua vez, encontra abrigo num dos fundamentos do nosso Estado Democrático de Direito, previsto em seu art. 1º, inciso III, qual seja, a dignidade da pessoa humana.

Além da fundamentabilidade reconhecida pela Emenda Constitucional nº115, entende-se que o direito à proteção de dados passa a integrar as cláusulas pétreas (art. 60, § 4º, inciso IV, da Constituição) e, portanto, imunes a qualquer supressão de seu predicado normativo, uma vez que seu conteúdo axiológico ressalta valores já protegidos pela Constituição Federal de 1988.

Tal entendimento é confirmado, entre outros, por Paulo Gonet Branco (2017) que esclarece sobre a possibilidade de declaração de novos direitos fundamentais via Emenda à Constituição de 1988 e aduz que a inclusão como cláusula pétrea

poderá ocorrer em se tratando de realçar um direito previamente existente, depreendida de regra mais abrangente da Constituição inaugural, como entende-se ser o caso da proteção de dados pessoais.

A proteção da dignidade da pessoa humana envolve todos os aspectos do indivíduo, sem exceção. Desse modo, deve ser incluída a proteção de dados como um componente do microssistema do ambiente digital tutelada pelo princípio.

Inicialmente, parece difícil estabelecer um conceito de dignidade, pois a concepção de digno e indigno pode variar em razão da cultura de cada sociedade, dos costumes, do sentimento de injustiça que aflora diante de um caso concreto etc.

No entanto, ela deve ser considerada como uma qualidade intrínseca e diferenciadora de cada ser humano, tutelando-o contra qualquer abordagem infamante e segregação abominável, assim como garante condições materiais mínimas de sobrevivência. É uma particularidade que toda pessoa tem, pois refere-se à sua condição humana. (RAMOS, 2014, p. 74)

No microssistema do ambiente digital pode-se afirmar que uma pessoa merece total e irrestrita proteção à sua dignidade, seja essa tutela em relação à função profissional que desempenha, à sua imagem perante seus pares, à sua intimidade, à sua privacidade e à proteção de seus dados pessoais.

Acresce-se à sua integridade física e psíquica o respeito ao seu pensamento, comportamento, sua imagem, intimidade, consciência e suas ações também no ambiente digital.

A dignidade humana é um valor absoluto e que, portanto, impossibilita questionamentos em relação à sua natureza. (COSTA, 2004, p. 14)

A dignidade é intrínseca ao ser humano e o respeito a ela é uma forma extrínseca de reconhecimento a esse direito.

Em especial no microssistema do ambiente digital, as disposições de um ordenamento jurídico não devem se dirigir somente aos Estados, mas também aos indivíduos, e elas devem ser aplicadas de forma que se possa atingir o bem-estar do ser humano, promovendo sua educação no meio social, pois a pessoa é possuidora de direitos subjetivos e detentora de valores que merecem consideração.

Observando que os textos constitucionais devem ser compreendidos como um sistema que seleciona determinados valores sociais, pode-se afirmar que a Constituição Federal brasileira elege a dignidade da pessoa humana como valor essencial que lhe dá unidade de sentido.

Além disso, é um dever social a aplicação concreta do princípio constitucional da dignidade da pessoa humana no microssistema do ambiente digital porque ele é o núcleo axiológico do direito contemporâneo nacional, o núcleo exegético do ordenamento jurídico brasileiro, o núcleo essencial de irradiação dos direitos humanos, o núcleo de proteção do ambiente digital e o fundamento da República Federativa do Brasil.

O princípio da dignidade da pessoa humana é o núcleo axiológico do direito contemporâneo nacional, o que significa afirmar que ele designa valor às normas jurídicas brasileiras.

Também é considerado como o núcleo exegético do ordenamento jurídico brasileiro, pois o raciocínio interpretativo de todas as regras deve se orientar pelo princípio, já que relações jurídicas humanas são fragmentárias e evoluem continuamente.

Igualmente, é preciso lembrar que o princípio da dignidade da pessoa humana constitui um núcleo essencial de irradiação dos direitos humanos, pois sua função é propagar os interesses fundamentais dos indivíduos.

Em outras palavras, pode-se afirmar que o epicentro de onde se irradiam quaisquer outros direitos fundamentais é o princípio da proteção da dignidade da pessoa humana, sendo que todos os demais princípios se desenvolvem como uma espiral, a partir daquele princípio nuclear.

O princípio da dignidade da pessoa humana é o núcleo de proteção do ambiente digital porque tutela os dados pessoais em todas as suas formas, incluindo os meios digitais.

Sob a análise legal, releve-se que a Constituição Federal de 1988 prevê a dignidade da pessoa humana no art. 1o, III, como fundamento da República Federativa do Brasil.

A dignidade é o primeiro alicerce do meio ambiente digital e a última armadura de acolhimento da tutela dos dados pessoais.

Esse fundamento não é estático, mas dinâmico, uma vez que proporciona o emprego de condições de vida em conexão com um piso vital mínimo de existência do ser humano.

Tem-se, no princípio da dignidade da pessoa humana, uma restrição ao poder político supremo de um Estado, pois, apesar de sua personalidade independente e autoridade plena, sua atuação esbarra na condição humana.

A dignidade da pessoa humana, um dos fundamentos da República Federativa do Brasil, apresenta-se como direito de proteção individual em relação ao Estado e aos demais indivíduos e como dever fundamental de tratamento igualitário dos próprios semelhantes no meio digital e fora dele.

Por fim, é importante destacar que o princípio da dignidade da pessoa humana também tutela a inclusão digital, que tem sido um assunto muito propalado nas preleções políticas e econômicas em razão da inserção das tecnologias de informação e comunicação, que interligam os integrantes da sociedade em pouquíssimo tempo. (MALHEIRO, 2016, p. 227)

No âmbito infraconstitucional, a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 constitui o eixo central desse microssistema, conforme desenvolveremos adiante que, inclusive, permite a interação, entre outros com o próprio microssistema da tutela dos interesses transindividuais, diante do que dispõe o seus arts. 22 e 42, § 3º.

A proteção de dados pessoais não fica adstrita ao critério da especialidade da norma da referida Lei Geral de Proteção de Dados, até porque, no ano de 2022, a proteção de dados foi alçada à condição de garantia constitucional do cidadão, cuja constituindo a dignidade da pessoa humana um dos fundamentos da República Federativa do Brasil.

Um diálogo com outras fontes normativas já se encontra estabelecido, sendo certo que a legislação que disciplinará a utilização da inteligência artificial encontrará esse ambiente e com ele deverá se integrar, afinal, a inteligência artificial deve sua existência à existência e tratamento de dados. É tributária direta da massiva e exponencial coleta de dados, mormente dados pessoais, que através de algoritmos programados para determinada finalidade produzem relações estatísticas aptas para fazer predições com elevada probabilidade de acerto.

Apenas para exemplificar este diálogo, a Lei Geral de Proteção de Dados, tem sua raiz no inciso LXXIX do art. 5º da Constituição Federal, mas disciplina temas intimamente relacionados com a Lei 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Ressalte-se que o referido Marco Civil da Internet inovou o ordenamento jurídico brasileiro especialmente no que diz respeito à atribuição da responsabilidade dos provedores da internet por ato de terceiro, que se tornou cada vez mais comum diante da possibilidade de acesso a conteúdo ilícito e ofensivo. Em prol da liberdade de expressão, seu art. 19 entendeu por bem responsabilizar o

provedor de aplicações somente em caso de inércia para retirar conteúdo ofensivo do ar após intimação judicial.

Mantém diálogo com o já referido Código de Defesa do Consumidor, com a Lei da Ação Civil Pública, sempre que se considera a proteção coletiva de dados, conforme já referido

No mesmo sentido, com relação à proteção de dados pessoais no ambiente digital e considerando a assimetria informativa, entende-se, por exemplo, ser plenamente aplicável a teoria do diálogo das fontes para se utilizar o conceito de vulnerabilidade informacional e técnica do Código de Defesa do Consumidor às pessoas naturais (titular dos dados) com relação ao consentimento fornecido aos agentes (controlador e operador) para tratamento de seus dados pessoais, a fim de equalizar o deslinde da relação jurídica entre as partes, uma vez que a Lei Geral de Proteção de Dados dispõe que um de seus fundamentos é a defesa do consumidor(art. 2, inciso VI), conforme aduz Macedo (2022, p. 670).

Como afirma Mendes (2016, p. 7): "o direito básico do consumidor à proteção de dados pessoais envolve uma dupla dimensão: (i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face de coleta, processamento, utilização e circulação dos dados pessoais; e (ii) a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade".

Portanto, a proteção de dados individuais, inclusive pelos meios digitais, também encerra vertente transindividual típica da sociedade massificada em que vivemos e não equivale nem a interesses privados, nem a interesses públicos, permanecendo entre ambos na modalidade de interesses sociais coletivos, conforme regramento do Código de Defesa do Consumidor.

Cabe observar que não obstante a regra do art. 3º, § 2º do referido Código apregoar sua aplicação aos serviços colocados no mercado mediante remuneração, fato é que diversos serviços oferecidos pela internet como se fossem gratuitos ao

consumidor (exemplo: e-mails; hospedagem de blogs etc.) são remunerados via publicidade e propiciados pela coleta de dados de navegação digital do usuário para a formação de perfis informacionais que permitirão identificar seus hábitos e preferencias de consumo.

Mas não é só. Mantém diálogo também com a Lei Brasileira de Inclusão (Lei nº 13.146, de 6 de julho de 2015), considerando que referida lei determina a remoção de obstáculos (barreiras) que promovam qualquer forma de discriminação.

Cabe lembrar a doutrina de Antonio Herman Benjamin e Claudia Lima Marques (2018, p. 29), quanto à aplicabilidade da teoria do diálogo das fontes, sobretudo porque a proteção de dados pessoais é um valor fundamental, conforme dispositivo constitucional anteriormente referido:

> A teoria do diálogo das fontes tem direta relação com os direitos fundamentais, pois põe em relevo o sistema de valores que estes representam e orienta a aplicação simultânea de regras de diferentes fontes para dar efetividade a estes valores.

Inobstante a aplicação simultânea de regras de fontes diversas, entende-se que a interpretação que se pretende levar a efeito deve ter um liame axiológico nítido entre as fontes conjugadas, não se avalizando a pretensão de estabelecer um elo casual entre searas jurídicas distintas e incompatíveis (BENJAMIN; MARQUES, 2018, p.30).

Os autores exemplificam que o referido Marco Civil da Internet dialoga com o Código de Defesa do Consumidor (CDC), pois estabelece princípios e garantias, direitos e deveres para o uso da internet no Brasil e esclarece ser um de seus fundamentos a defesa do Consumidor (art. 2º, inciso V) (BENJAMIN; MARQUES, 2018, p.38).

Quando se cogita da aplicação simultânea de fontes, não se deve olvidar que para a criação de um microssistema de proteção de dados pessoais, a Constituição deve ser considerada como sistema.

A Constituição Federal de 1988 é um sistema aberto e em interação com o ecossistema social no qual foi gerada.

Logo, se a ordem constitucional é um sistema, posto que apresenta uma conexão de princípios expressos e implícitos, caracterizadores de uma unidade e ordem tendentes à organização dos elementos constitutivos do Estado de Direito, todo e qualquer microssistema deverá nortear-se de acordo com as normas constitucionais.

Assim, as fontes normativas infraconstitucionais deverão comunicar-se de forma a constituir-se em uma unidade sistemática, seguindo as lições de Konrad Hesse que afirma que:

> la Constitución solo puede ser comprendida e interpretada correctamente cuando se la entiende, en este sentido, como unidad, y que el Derecho Constitucional se halla orientado en mucha mayor medida hacia la coordinación que no hacia el deslinde y el acotamiento (1983, p. 18).

Portanto, o microssistema de tutela de proteção de dados que aqui se pretende fixar como doutrina, deverá ser construído e alicerçado sobre os aspectos axiológicos da Constituição Federal de 1988, em razão de sua força normativa (HESSE, 1991).

Em relação ao proposto acima mencionado, a restrição à atividade exegética da Lei Geral de Proteção de Dados também encontra fundamento ao relacionar a temática proteção de dados no âmbito penal.

A tutela de dados pessoais deve partir do reconhecimento de que o tema transcende a vertente do Código Penal, no qual a proteção é prevista de maneira individualista e tradicional. Portanto, a proteção de dados pessoais além da proteção da Lei Geral de Proteção de Dados deve encontrar acento significativo em uma tutela criminal difusa. Claro é que não se pretende esvaziar o conteúdo principiológico do Direito Penal e Processual Penal clássico, mas observar que os Códigos tradicionais assimilam a ótica da dicotomia dos direitos públicos e privados.

Ao deparar-se com a proteção de dados pessoais, observa-se que a tutela vai além de bens jurídicos individuais, passando à valoração destes em observância a direitos que atingem subsistemas sociais, econômicos, culturais.

Sobre o tema, Winfried Hassemer bem expõe que a "moderna legislação penal move-se segundo um conceito político criminal ambivalente: de um lado existe uma prudente descriminalização no âmbito do Direito Criminal 'clássico', enquanto em outro, há um processo de criminalização de comportamentos ofensivos a bens jurídicos universais (coletivos)" (1985, p.367).

Assim, ao deparar-se interesses difusos, como são os dados pessoais (levando-se em consideração, sobretudo a sua essencial indivisibilidade), a tutela criminal deve ser difusa sustentando-se a ideia da necessidade de um microssistema a ser pensado segundo o princípio da dignidade da pessoa humana como fundamento da República Federativa do Brasil que se constitui em Estado Democrático de Direito.

Portanto, os dados pessoais consistem em bens jurídicos que devem ser penalmente tutelados, por meio de um microssistema que garanta efetividade e caráter ético e antropocêntrico ao uso das novas tecnologias.

Sobre o tema, Figueiredo Dias (1999, p. 74) afirma a importância da tutela dos interesses metaindividuais para o Direito Penal:

> Uma convicção que só se reforçará recusando- como se deve recusar- uma ilegítima restrição da noção de bens jurídico-penais a interesses puramente individuais e ao seu encabeçamento em pessoas singulares, e aceitando antes a plena legitimidade da existência de bens jurídicos transpessoais, coletivos, comunitários ou sociais. É, em meu juízo, no aprofundamento e esclarecimento do estatuto dessa classe de bens jurídicos – cujo reconhecimento, de resto, não afetará a natureza em última instância "antropocêntrica" da tutela penal- que reside, no futuro próximo, a tarefa primária da doutrina (...)

A partir da noção do Estado Democrático de Direito, os mandados de criminalização encontram sua razão valorativa e permissiva, sendo instrumentos do sistema constitucional que objetivam a proteção de direitos fundamentais. Em

sendo a tutela da proteção de dados um bem jurídico relevante e fundamental à existência digna do ser humano, a ordem de criminalização em um microssistema encontra respaldo na força normativa da Constituição.

A construção doutrinária que se propõe entende, portanto, que a a proteção de dados pessoais não está restrita à Lei Geral de Proteção de Dados. Em verdade a exegese deve ir ao encontro de se estabelecer um diálogo com outras fontes normativas compatíveis, a fim de relacionar a legislação à luz de vetores coerentes e complementares para conformá-la à realidade e aos direitos fundamentais.

A inteligência artificial deve sua existência ao tratamento de dados. É tributária direta da massiva e exponencial coleta de dados, mormente dados pessoais, que através de algoritmos programados para determinada finalidade produzem relações estatísticas aptas para fazer predições com elevada probabilidade de acerto.

A um só tempo, devem ser protegidos, diante da garantia constitucional referida, e constituem produto de tratamento, conforme a disciplina da Lei Geral de Proteção de Dados que em seus (65) sessenta e cinco artigos emprega a palavra "tratamento" mais de uma centena de vezes.

A utilização da inteligência artificial pressupõe o tratamento de dados.

Portanto, os projetos de lei sobre utilização da inteligência artificial e sobre as denominadas "fake news" encontrarão um ambiente legislativo que observa essas garantias.

A legislação ainda deverá considerar, para que se integre a esse microssistema à proibição de qualquer forma de se erigir as denominadas "barreiras atitudinais"; assim, a eliminação de barreiras atitudinais trata da compreensão da diversidade em diversos âmbitos, gênero, orientação sexual, deficiências, raça, religião etc. e no contexto aqui tratado, para o âmbito do ambiente digital.

Trata-se de um tema que, a despeito de estar disciplinado na Lei Brasileira de Inclusão, anteriormente referida, não se destina exclusivamente à proteção exclusiva das pessoas com deficiência.

Constitui um conceito que deve ser utilizado contra quaisquer formas de discriminação, inclusive as potencialmente criadas pela inteligência artificial.

A Lei Brasileira de Inclusão (Lei Nacional nº 13.146, de 6 de julho de 2015), está lei em vigor no Brasil garante os direitos das pessoas com deficiência e impõe as penalidades a quem infringir a lei e é clara ao definir como barreira atitudinal as atitudes ou comportamentos discriminatórios, que impeçam a inclusão das pessoas ou, dito de outra forma, que promovam qualquer tipo de discriminação.

A inteligência artificial não poderá expressar as atitudes e comportamentos de quem a idealiza.

Acrescente-se, ainda, que o tratamento de dados, principalmente para a utilização da inteligência artificial que, de alguma forma, classificará as pessoas (vedada a classificação para fins discriminatórios e/ou de exclusão), invariavelmente tratará dados que podem ser classificados como difusos, coletivos em sentido estrito, ou individuais homogêneos, fato que integra esse microssistema ao anteriormente referido, considerando que, se necessária a judicialização de um conflito, seja previamente verificado se a tutela jurisdicional coletiva é a que deve ser empregada, inclusive conforme referido anteriormente, sob o âmbito do direito penal. Claro é que em relação ao último ponto, resta muito importante significar a necessidade do microssistema na ótica penal no campo das novas tecnologias e, em especial, da inteligência artificial, não apenas para criar crimes, autores de delitos determinados e vítimas específicas, responsabilidades, afastando-se dos princípios do Direito Penal Codificado, mas com o objetivo de tutelar bens jurídicos historicamente construídos em face da sociedade da informação (prospectando a construção da tipificação criminal difusa baseada em dois fundamentos: a) dignidade criminal ; b) carência criminal (DOLCINI; MARINUCCI,1994, p. 156).

6. Responsabilidade civil.

Neste passo vale indagar, na esteira do pensamento do professor do Instituto de Ciência e Tecnologia da Unesp e ex-integrante do Comitê Especial para Inteligência Artificial da Sociedade Brasileira de Computação, Alexandre Simões, que, analisando o PL nº 21/2020, questionava a respeito de quem deve ser responsabilizado nas situações que resultem em acidentes envolvendo automóveis autônomos, por exemplo? "o fabricante do carro, o do software, ambos, ou nenhum deles"?

O tema é certamente polêmico e provocará, como de fato já provoca, debates acalorados, semelhantes aos que foram levados a efeito por ocasião da criação, em agosto de 2001, da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), e, mais recentemente, da Lei Geral de Proteção de Dados, especialmente com relação a esta última, em face da norma do art. 20 que retirou a possibilidade de as revisões das "decisões tomadas unicamente com base em tratamento automatizado de dados pessoais" serem realizadas por pessoas naturais, como originalmente previsto.

Considerando os riscos que a utilização cada vez mais frequente de algoritmos inteligentes em quase todos os setores da atividade humana acarreta, a questão que se coloca é a da responsabilidade civil aplicável à inteligência artificial.

Dentre as teorias criadas para explicar a existência dos referidos riscos: risco proveito; risco profissional; risco excepcional; risco integral; e risco criado, essa última, como aduz Caio Mário da Silva Pereira (1993, p. 268), estabelecendo que "se alguém põe em funcionamento uma qualquer atividade, responde pelos eventos danosos que esta atividade gera para os indivíduos, independentemente de determinar se em cada caso, isoladamente, o dano é devido à imprudência, à negligência, ou a um erro de conduta", parece ser a de maior aceitação.

A bem da verdade, a teoria do risco criado parece também ser a predileta do Parlamento Europeu posto que, no item 8 do anexo B da Proposta do Regime

de responsabilidade civil aplicável à IA, que integra o conjunto de documentos que compõem a Resolução de outubro de 2020, referido Parlamento, após reconhecer "que o tipo de sistema de IA sobre o qual o operador exerce controle é um fator determinante para a atribuição de responsabilidade", sustenta que deverá ser sempre claro que quem cria

> [...] mantém, controla o sistema de IA, ou nele interfere, deverá ser responsável pelos danos ou prejuízos causados pela atividade, o dispositivo ou o processo. Tal resulta de conceitos jurídicos gerais e amplamente aceites em matéria de responsabilidade, segundo os quais a pessoa que cria ou mantém um risco para o público é responsável se esse risco causar dano ou prejuízo e, por conseguinte, deverá minimizar a priori ou compensar a posteriori esse risco. Consequentemente, a ascensão dos sistemas de IA não implica uma revisão completa das regras em matéria de responsabilidade em toda a União. Para responder aos desafios relacionados com a IA, seria suficiente proceder a ajustamentos específicos da legislação existente e introduzir disposições novas bem avaliadas e orientadas, com vista a evitar a fragmentação regulamentar e a garantir a harmonização da legislação em matéria de responsabilidade civil em toda a União no que toca à IA.

Em conformidade com a teoria do risco criado, que é uma ampliação da teoria do risco proveito, qualquer atividade, seja econômica ou não, é geradora de riscos, isto é, o agente coloca-se em situação de risco tão somente por exercer a atividade e, portanto, estará obrigado a indenizar bastando a exposição ao dano.

Eugênio Facchini Neto assevera que:

> Dentro da teoria do risco-criado, destarte, a responsabilidade não é mais a contrapartida de um proveito ou lucro particular, mas sim a consequência inafastável da atividade em geral. A ideia de risco perde seu aspecto econômico, profissional. Sua aplicação não mais supõe uma atividade empresarial, a exploração de uma indústria ou de um comércio, ligando-se, ao contrário, a qualquer ato do homem que seja potencialmente danoso à esfera jurídica de seus semelhantes. Concretizando-se tal potencialidade, surgiria a obrigação de indenizar. (2023, p. 71-108)

Em razão de sua natureza ou dos elementos utilizados, algumas atividades sujeitam o ser humano a todo tipo de risco e, em consequência, deve assumir os resultados advindos dessas atividades. Deste modo, toda pessoa que, em virtude do exercício de uma atividade, profissional ou não profissional, gera um risco inerente, ficará sujeita a reparar danos que eventualmente venham a decorrer.

No mesmo sentido, leciona Sergio Cavalieri Filho, ao afirmar que, na doutrina do risco criado:

> ...independentemente da culpa, e dos casos especificados em lei, haverá obrigação de reparar o dano quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, riscos para os direitos de outrem. (2007, p. 154)

Feitas as breves considerações supra, parece evidente que qualquer proposta legislativa tendente a regulamentar a inteligência artificial deverá, necessariamente, considerar, nesse ambiente, a responsabilidade civil dos envolvidos na cadeia produtiva, desde a criação até a comercialização.

7. Reflexões conclusivas,

Analisados todos esses elementos, observa-se, de forma inquestionável a existência de fundamentos suficientes a autorizar a conclusão de que, na atualidade, contamos com um microssistema jurídico apto para cuidar do ambiente digital, contendo (i) lei especial estruturante (LGPD, lei 13.709/18); (ii) princípios básicos novos e específicos, como o da autodeterminação informativa (art. 2, II); e (iii) institutos próprios, como por exemplo a noção de dado pessoal sensível (art.5, II) e o tratamento de dados (art. 5, X).

Nossas pesquisas prosseguirão e traremos novas e complementares reflexões sobre o tema, aperfeiçoando-o para tratar de forma adequada a complexidade das relações sociais advindas com as novas tecnologias, a fim problematizar a acomodação de novos textos normativos compatíveis, como certamente deve ocorrer com a legislação referentes aos usos e aplicação de Inteligência artificial a fim de integrá-los ao microssistema do ambiente digital.

Referências preliminares – 1ª Edição

BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). O Direito na Sociedade da Informação. São Paulo: Atlas, 2007.

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima. A Teoria do Diálogo das Fontes e seu Impacto no Brasil: uma homenagem à Erik Jayme. Revista de Direito do Consumidor, São Paulo, v. 115, ano 27, jan./fev. 2018. Disponível em: https:// revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1042/911. Acesso em: 16 fev. 2022.

BRANCO, Paulo Gustavo Gonet. Cláusulas pétreas. Enciclopédia jurídica da PUC-SP. In: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (coord.). Tomo: Direito Administrativo e Constitucional. NUNES JR., Vidal Serrado; ZOCKUN, Maurício; ZOCKUN, Carolina Zancaner; FREIRE, André Luiz (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/21/edicao-1/clausulas-petreas. Acesso em: 16 fev. 2022.

CAVALIERI FILHO, Sergio. Programa de Responsabilidade Civil. 7. ed. São Paulo: Atlas, 2007.

Costa, Tailson Pires. Dignidade da pessoa humana diante da sanção penal. São Paulo: Fiúza, 2004.

DOLCINI, Emílio; MARINUCCI, Giorgio. Constituição e escolha dos bens jurídicos. Revista Portuguesa de Ciência Criminal. Lisboa. Abril/junho 1994.

FACCHINI NETO, Eugenio. ANDRADE, Fábio Siebeneichler de. Reflexões sobre o modelo de responsabilidade civil para a inteligência artificial: perspectivas para o direito privado brasileiro. In: Gabrielle Bezerra Sales Sarlet et al. (Org.). Inteligência artificial e direito. 1ed.Porto Alegre: Fundação Fênix, 2023, v. 1.

FIGUEIREDO DIAS, Jorge de. Questões fundamentais do Direito Penal revisitadas. São Paulo: RT, 1999.

HASSEMER, Winfried. Spunti per una discussionesud tema bene giuridico e riformadella parte speciale. In: Alfonso M. Stile. Bene giuridico e riformadella parte speciale, 1985.

HESSE, Konrad. Escritos de Derecho Constitucional . Centro de Estudios Constitucionales, Madrid, 1983.

HESSE, Konrad. Força Normativa da Constituição. Trad. Gilmar Ferreira Mendes. Porto Alegre: Fabris, 1991.

MACEDO, C. S. Direito fundamental à proteção de dados pessoais: necessário reprimir a normatividade tecnológica da economia digital. Revista Jurídica da Presidência, Brasília, Volume 24, Número 134, Set/Dez, 2022.

MENDES, L. S. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. Revista de Direito do Consumidor, 105, 1-30, 2016.

MALHEIRO, Emerson Penha. Direitos humanos nasociedade da informação. São Paulo: Revista Paradigma, 2016. Disponível em: https://revistas.unaerp.br/paradigma/article/view/2. Acesso em: 13 jun. 2023.

RAMOS, André de Carvalho Ramos. Curso de direitos humanos. São Paulo: Saraiva, 2014.

SENISE LISBOA, Roberto. Direito na sociedade da informação. Revista dos Tribunais, v. 95, n. 847, 2006.

TAKAHASHI, Tadao. Sociedade da informação no Brasil: livro verde. Ministério da Ciência e Tecnologia (MCT), 2000.

VIEIRA, Oscar Vilhena; POPPOVIC, MalakelChichini. Perspectivas sobre o Movimento Internacional de Direitos Humanos no Século XXI: as respostas mudam. IN: Revista SUR. N. 20. São Paulo: Conectas Direitos Humanos, 2014.

II – DESENVOLVIMENTO

CONTORNOS NUCLEARES DO MICROSSISTMA JURÍDICO DO AMBIENTE DIGITAL NA LEGISLAÇÃO BRASILEIRA

Caio Sperandeo de Macedo

Introdução:

O propósito do presente estudo é ratificar a proteção de dados pessoais, inclusive nos meios digitais, enquanto direito fundamental na Constituição Federal de 1988, bem como identificar os requisitos configuradores de um microssistema jurídico autônomo para o ecossistema digital fulcrado na Lei nº13.709/2018-LGPD, considerada como norma estruturante e que deve ser conjugada com outras leis especiais aplicáveis, notadamente a legislação que cuida dos direitos transindividuais e a futura legislação sobre a aplicação e os usos da inteligência artificial em nosso país, uma vez que esta nova tecnologia se baseia na coleta e no tratamento de dados.

A priori, a concepção do microssistema jurídico do ambiente digital parte da gênese da constitucionalização do direito à autodeterminação informativa a rogo Emenda Constitucional nº115/2022, que introduziu o inciso LXXIX ao artigo 5º, CF/88, a fim de garantir a proteção de dados pessoais, inclusive nos meios digitais, concebendo uma nova nuance à dignidade da pessoa humana.

Acrescentando-se a tal previsão constitucional o alcance da proteção jurídica ofertada pela Lei Geral de Proteção de Dados Pessoais (LGPD) em complemento com outras fontes compatíveis e complementares como a Lei de Acesso à

Informação (Lei 12.527/2011, por ex. art. 4, IV e V; art. 7, III; art. 31, §5º), A Lei do Cadastro Positivo (Lei 12.414/2011, por ex.: art. 2º, I), o Marco Civil da Internet (Lei 12.965/2014, por ex.: art. 3º, III e seu parágrafo único; art. 7, VIII, art. 11) e especialmente a legislação que cuida dos direitos transindividuais (Lei 8.078/90, art. 4, I, II e III, 6, VIII, art. 7, art. 43, 81 etc).

Entende-se que há um elo epistemológico entre a proteção de dados pessoais e o diploma que cuida dos direitos transindividuais, uma vez que ambos compartilham características de direito coletivo lato sensu do azo que tanto a proteção de dados como a Lei 8.078/90 costumam tratar de violações com muitas vítimas; com pluralidade de causas e de múltiplos atores, e enfrentam a dificuldade de identificar as violações a direitos e delimitar as responsabilidades.

E ao pugnar pela existência do microssistema jurídico autônomo para o ambiente digital indicando como lei estruturante a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), não nos desincumbiremos da tarefa de apontar seus princípios específicos inovadores e conceitos-chave que lhe dão identidade própria.

Neste contexto, esclarecer de que forma é possível considerar a LGPD como norma estruturante para cuidar da proteção de dados pessoais em diálogo com outras fontes normativas. E comprovar que, salvo outro juízo, a LGPD ostenta todos os requisitos técnicos (abrange normas de direito material, processual, bem como de direito público e privado) aplicáveis às relações jurídicas sobre a proteção de dados pessoais, o que habilita tal norma a funcionar como lei estruturante para o microssistema jurídico autônomo voltado para a proteção de dados pessoais no ambiente digital.

A proteção de dados pessoais sobre o enfoque de um microssistema jurídico autônomo ganha relevo não só por se entender presentes seus requisitos configuradores, mas, principalmente, porque permitirá acomodar de forma sistemática e confere maior segurança jurídica à futura legislação sobre os usos e

aplicação da inteligência artificial ainda em discussão no Senado Federal de nosso país diante da relação entre a coleta de dados pessoais e o treinamento de algoritmos.

1. A Lei 13.709, de 2018(LGPD) e a interação com a teoria do diálogo das fontes

O reconhecimento do direito à autodeterminação informativa como garantia fundamental via Emenda Constitucional nº115/2022 (a qual acrescentou o inciso LXXIX ao artigo 5º, CF, dispondo que: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"), ratificou posicionamento anterior do Supremo Tribunal Federal, no julgamento da ADI-STF nº6387[1] e se consubstanciou em um passo determinante no processo de consolidação da proteção de dados pessoais em nosso país.

A LGPD representa um novo paradigma na legislação que pretende tutelar o uso de dados pessoais, mormente os dados considerados sensíveis, que em linhas gerais veda o uso indiscriminado de dados dos titulares, pessoas físicas, e estabelece políticas de proteção para garantir a autodeterminação informativa enquanto direito ligado à personalidade, a quem os dados coletados fazem referência (Stelzer, Et. Al, 2019, p.02).

Ivo Wolfgang Sarlet (Sarlet, 2022) reforça tal relevância não apenas para a compreensão do conteúdo e alcance do direito fundamental à proteção de dados pessoais na CF/88, mas também para efeitos de seu diálogo com a legislação, jurisprudência e doutrina sobre o assunto, esclarecendo que outros diplomas

[1] ADI 6387 MC-REF/DF- Trecho destacado da Ementa(07/05/2020): [...] "1.Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art.5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos."[...]. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso: 17.Jul.2023.

normativos já dispõem sobre aspectos da proteção de dados, exemplificando com a Lei de Acesso à Informação (Lei 12.527/2011), o Marco Civil da Internet (Lei 12.965/2014) e notadamente a LGPD (Lei 13.709, de 2018).

Neste último caso, consigne-se que a Lei Geral de Proteção de Dados(Lei nº13.709/2018), inovou ao trazer conceitos específicos, como por exemplo: em seus princípios (art 1º); nos fundamentos (art 2º); na noção do consentimento do titular (art. 7º); que o tratamento de dados pessoais deverá observar a boa-fé e demais vetores principiológicos (art 6º, incisos de I a X); na definição do legítimo interesse do controlador (art. 10); do momento de término do tratamento de dados (art. 15); no tratamento de dados considerados como sensíveis (art. 17); nos direitos do titular de dados (art. 18); no direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20); na defesa dos interesses e dos direitos dos titulares de dados exercidos em juízo, individual ou coletivamente (art. 22); no tratamento de dados pelo poder público (art. 23); na responsabilidade e ressarcimento por danos patrimoniais, morais, individuais ou coletivos (art 42) etc..

Assim, a legislação sobre tratamento de dados pessoais, inclusive no ambiente digital, pretende regular assunto complexo tendo por certo que abarca relações jurídicas de direito individuais e pode-se dizer predominantemente de caráter coletivo lato sensu, o que demanda a necessidade de interpretá-las consoante os valores que efetivem a concretização de direitos fundamentais ali albergados como o da privacidade, liberdade, desenvolvimento da personalidade, autodeterminação informativa, dignidade da pessoa humana.

Neste panorama, Rafael A. F. Zanatta (2019, p.202-203) reforça que se faz necessário entender a proteção de dados pessoais pela perspectiva de direito coletivo, uma vez que a dinâmica social das múltiplas relações telemáticas

cotidianas inviabiliza que racionalmente os indivíduos tenham pleno conhecimento de todas as relações jurídicas assumidas diante das inúmeras oportunidades em que teve os dados pessoais coletados (Zavaglia Coelho, Et. Al, 2023 p.19), que muitas vezes *não* foram obtidos mediante consentimento esclarecido para a finalidade determinada (LGPD, art. 5, XII).

Sugere referido autor (Zanatta, 2019, p. 205) que a coletivização da proteção de dados deve predominantemente ser tutelada por entidades civis especializadas com legitimidade para propositura de ações civis públicas, nisso incluído o Ministério Público (129 CF/88) e, também, demais entidades e órgãos da administração pública voltados à defesa dos direitos e interesses difusos e coletivos.

Ademais, o art. 22, combinado com 42, §3º, ambos da LGPD, asseguram respectivamente: que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente na forma do disposto na legislação pertinente, utilizando-se dos instrumentos de tutela individual e coletiva (art. 22); e que as ações de reparação por danos coletivos podem ser exercidas coletivamente em juízo, observada a legislação pertinente (art. 42, §3º).

Pontua Erik Jayme (2000, p.66) sobre a importância da teoria do diálogo das fontes como forma de extrair efeitos jurídicos mais precisos de direitos fundamentais oriundos de direitos humanos:

> O 'diálogo das fontes' significa, que decisões de casos da vida complexos são hoje o somar, o aplicar conjuntamente, de várias fontes (Constituição, Direitos Humanos, direito supranacional e direito nacional). Hoje não mais existe uma fixa determinação de ordem entre as fontes, mas uma cumulação destas, um aplicar lado a lado. Os direitos humanos são direitos fundamentais, mas somente as vezes é possível deles retirar efeitos jurídicos precisos.

Complementando com o escólio de Antonio Herman Benjamin e Claudia Lima Marques (2018, p. 29), quanto à aplicabilidade da teoria do diálogo das fontes, eles esclarecem que:

> A teoria do diálogo das fontes tem direta relação com os direitos fundamentais, pois põe em relevo o sistema de valores que estes representam e orienta a aplicação simultânea de regras de diferentes fontes para dar efetividade a estes valores.

Salientam ainda, referidos autores, que a aplicação simultânea de regras de fontes diversas deve ter um liame axiológico nítido, não se compactuando com a pretensão de estabelecer um elo casual entre searas jurídicas distintas e incompatíveis (Benjamin; Marques, 2018, p.30).

Além dos diplomas referidos acima por Sarlet (2022), reputamos necessário acrescentar que a LGPD (especialmente art 2º, VI; artigo 18 §8º, art. 22, e art. 42, §3º) também estabelece diálogo construtivo com a legislação consumerista (LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990) e seus instrumentos e mecanismos de tutela específica quando o caso envolver relações transindividuais.

Estamos a falar de um diálogo sistemático de coerência, em que, na aplicação simultânea de duas normas, a primeira (lei "A") funciona como base teórica para a segunda (lei "B"), uma vez que aquela (lei "A") é a lei estruturante do assunto relacionado à proteção de dados (no caso, a LGPD) e a outra (lei "B") um microssistema específico (no caso, o CDC) que se comunica subjetivamente para tutelar o regramento dos direito coletivos, transindividuais (Morais, 2019, p.151).

Tal diálogo entre a proteção de dados com a legislação que cuida dos direitos transindividuais ganha relevo quando é cediço que a coleta e tratamento de dados pessoais, mormente os considerados como sensíveis, é cada vez mais intensa na atual Sociedade de Dados (*Data Driven Economy*[2]) em decorrência de tecnologias de inteligência artificial em seus diversos usos e aplicações que dependem de acervo e tratamento de grande volume de dados para treinamento e performance

[2] Disponível em: https://www.intereconomics.eu/contents/year/2019/number/4/article/data-driven-economy-challenges-and-opportunities.html. Acesso em 15.fev.2023.

de algoritmos desenvolvidos entre outras funcionalidades para predição estatística de comportamentos que visam à perfilização de tendências e a influenciar hábitos de consumo.

Caso o tratamento de dados envolva relação de consumo, temos que dentre as disposições fundamentais do CDC, está aquela que determina a interpretação mais favorável ao consumidor (art. 47) de modo a equilibrar os interesses antagônicos, consoante jurisprudência com trecho de ementa em destaque:

> "2. (...) Ademais, tratando-se de relação de consumo, o consumidor é a parte vulnerável na demanda e, portanto, a interpretação da lei lhe deve ser feita de forma mais favorável."
>
> Acórdão 982993, 20160110098658APC, Relator: ROBSON BARBOSA DE AZEVEDO, Quinta Turma Cível, data de julgamento: 23/11/2016, publicado no DJE: 30/1/2017 [3].

Ademais, não se olvide que a futura legislação sobre inteligência artificial em nosso país, cujos projetos de lei, respectivamente: Projeto de Lei n° 2338, de 2023, Iniciativa: Sen. Rodrigo Pacheco (PSD/MG)[4] e Projeto de Lei 21/2020[5] Iniciativa: Dep. Eduardo Bismarck (PDT-CE), que estão em tramitação no Senado Federal, necessariamente deverá ser outra fonte a se relacionar com a LGPD, diante da ligação umbilical entre os temas.

A futura legislação prevendo a aplicação e usos da inteligência artificial[6] integrará naturalmente o que ora se denomina de microssistema jurídico do

[3] Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/cdc-na-visao-do-tjdft-1/principios-do-cdc/principio-da-interpretacao-mais-favoravel-ao-consumidor#:~:text=Dentre%20as%20disposi%C3%A7%C3%B5es%20fundamentais%20do,efetivo%2C%20os%20interesses%20do%20consumidor.Acesso em: 31. Jul. 2023.

[4] Disponível em: https://www12.senado.leg.br/noticias/audios/2023/05/marco-legal-para-inteligencia-artificial-e-apresentado-por-pacheco?_gl=1*xknsmr*_ga*ODg2MzIyOTI3LjE2ODk5NDQyODE.*_ga_CW3ZH25XMK*MTY4OTk0NDI4MC4xLjEuMTY4OTk0NDM4OS4wLjAuMA.. Acesso em 20 jul. 2023.

[5] Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340 . Acesso em 24 jul. 2023.

ambiente digital diante da relação de causa (coleta de dados) e efeito (tratamento de dados) entre àquela e a proteção de dados pessoais, conforme Macedo (et al., 2023, p.18):

> A inteligência artificial deve sua existência ao tratamento de dados. É tributária direta da massiva e exponencial coleta de dados, mormente dados pessoais, que através de algoritmos programados para determinada finalidade produzem relações estatísticas aptas para fazer predições com elevada probabilidade de acerto.

No mesmo sentido, para Christian Troncoso (Troncoso, 2022): "há trade-offs entre inovação de IA e proteção de dados", conforme notas explicativas 207[7] e 219[8], respectivamente:

> Então, sim, há uma interseção da proteção de dados e IA que levanta várias discussões, mas devemos reconhecer que inovação é importante, mas a proteção de dados também. [...] (p.136).

> [...] a regulação da IA não deve partir do zero, mas deve seguir a legislação existente que é neutra com relação à tecnologia, citando leis que protegem direitos civis e leis de proteção de dados. (p.140).

Impende destacar, ainda, que o artigo 7º do CDC [9] confere abertura para se

[7] RELATÓRIO FINAL - COMISSÃO DE JURISTAS RESPONSÁVEL POR SUBSIDIAR ELABORAÇÃO DE SUBSTITUTIVO SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4. Acesso: 11 out. 2023.

[8] RELATÓRIO FINAL - COMISSÃO DE JURISTAS RESPONSÁVEL POR SUBSIDIAR ELABORAÇÃO DE SUBSTITUTIVO SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4. Acesso: 12 out. 2023

[9] Art. 7° Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e eqüidade.

estabelecer diálogo subsidiário com outras fontes normativas interpretativas para o reconhecimento e proteção de direitos transindividuais, como a LGPD. Portanto, valores e princípios interpretativos oriundos do Direito do consumidor (por exemplo, o conceito de vulnerabilidade frente à assimetria informacional entre titular de dados e agentes de tratamento; de bem coletivo lato sensu; e mecanismos de tutela coletiva) também conferem guarida à proteção de dados pessoais quando envolver direitos e interesses indivisíveis.

2. Características de um Microssistema jurídico

A partir da década de 1970 fora observado o surgimento de microssistemas jurídicos autônomos diante da necessidade de atendimento de nova dinâmica na sociedade e da pluralidade de suas relações, o que impôs a ressignificação de conceitos normativos outrora estabelecidos ou a construção de novos paradigmas interpretativos, passando a exigir postura mais proativa dos operadores do Direito, a fim de contornar o árduo processo de revisão legislativa dos códigos, que têm por pretensão tratar exaustivamente determinado ramo do direito em um único texto legal.

Conforme aduz Pena (2007, p. 53), comentado análise de Natalino Irti com relação ao processo de formação do fenômeno dos microssistemas jurídicos verificados a partir de idos de 1970 em Itália:

> Irti percebia que as leis especiais passavam de fenômeno secundário e marginal, a fenômeno central; de normatização temporária e pontual a regulamentação permanente. E identificava uma pluralidade de microssistemas, encerrando as leis especiais, nascidas sob o signo da diferença, que, por sua reiteração e estratificação, tornavam-se capazes de exprimir princípios autônomos. Percebia o autor que essas leis especiais alcançavam certo grau de estabilidade e assumiam a forma de texto único ou lei orgânica, concebendo, então, a teoria dos microssistemas, como esforço de expansão da racionalidade sistemática às fronteiras do próprio ordenamento.

Aludido fenômeno jurídico foi igualmente observado no Brasil em décadas posteriores, uma vez surgindo a necessidade de edição de leis especiais focadas em temáticas específicas diante da insuficiência dos códigos para tratar de temas pontuais candentes na sociedade. Tal fato foi a gênese do que se passou a identificar de microssistemas jurídicos autônomos, do que são exemplos em nosso país o Estatuto da Criança e do Adolescente (LEI Nº 8.069, DE 13 DE JULHO DE 1990.) e o Estatuto do Idoso (LEI No 10.741, DE 1º DE OUTUBRO DE 2003.), Estatuto de Defesa do Torcedor (Lei nº 10.671, De 15 De MAIO De 2003) etc.

Para Xexéo (2018, p.1226), a pedra de toque de um microssistema jurídico é uma lei inaugural que traz uma nova dimensão para o respectivo assunto, para a qual os demais textos normativos devem dialogar, pois [...] ao "se teorizar a presença de novo microssistema tem-se que ter por base nova lei especial que traz nova ótica para o ordenamento, aglutinando as demais normas especiais a seu redor. [...]".

Tem a acrescentar Cervo (2014, p.83) que a característica de um microssistema reside na sua capacidade de abranger no mesmo diploma normas de direito material, processual, público e privado, aplicáveis às relações jurídicas de determinados grupos, minorias ou temas.

Já Marcelo de Melo Vieira (2020, p. 137) destaca como características de um microssistema a previsão do tema no âmbito do texto constitucional, além de referendar o tratamento multidisciplinar e a existência de lei específica.

Em termos operativos, Morais (2019, p. 144) faz alusão às vantagens de um microssistema quando comparado à sistemática da codificação, destacando dentre outros: (i) o tratamento sistemático a institutos antes dispersos no ordenamento jurídico; (ii) a maior segurança jurídica, uma vez que trazem regras específicas ou setoriais; (iii) a regulação minudente da matéria, trazendo normas de diversos ramos do direito no mesmo diploma normativo; (iv) a possibilidade de alteração legislativa

mais célere; e (v) a personalização das normas jurídicas, valorizando particularidades.

É de se ressaltar que o surgimento de um microssistema não altera a vigência ou a aplicabilidade dos demais que continuam operantes, do azo que o novo microssistema passa a conviver com os anteriores se inter-relacionando; não há relação de subordinação e, sim, de interdependência (Irti, 1998, p.70/72), uma vez que todos extraem seu fundamento de validade da força normativa da Constituição (Hesse, 1991).

Assim, ao densificar o projeto constitucional em determinados campos específicos, os microssistemas devem atender à necessidade de preservar o caráter sistêmico da ordem constitucional (Schreiber; Konder, 2016, p.22/23).

3. O Microssistema jurídico do ambiente digital e a proteção de dados

Como se depreende do exposto em linhas anteriores, os autores divergem com relação às características do que consideram que um microssistema jurídico deve apresentar para considerá-lo como autônomo. Adotamos para este estudo os requisitos ponderados por Xexéo (2018, p.1227) que identifica três elementos nucleares que devem estar presentes: (i) uma lei estruturante; (ii) novos princípios específicos; e (iii) institutos que lhe garantam identidade própria.

Assim, pode-se identificar de forma objetiva que o microssistema jurídico do ambiente digital que ora se propõe como autônomo em nosso ordenamento contém, além de guarida constitucional (art. 5º, inciso LXXIX da CF/88), os seguintes requisitos configuradores, a saber: (i) a referida lei especial estruturante, consubstanciada na LGPD, lei 13.709/18, cujos elementos foram destacados anteriormente; (ii) princípios básicos novos e específicos[10]; à guisa de exemplos

[10] Reiteramos posicionamento do STF na ADI 6387 MC-REF/DF- Trecho destacado da Ementa (07/05/2020): [...] "1.Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº13.709/2018 (Lei Geral de

referimo-nos ao da autodeterminação informativa, previsto pelo art. 2, II; ao da finalidade e ao da adequação, a rogo do Art. 6º, incisos I e II[11]; e com relação aos (iii) institutos próprios, servem de exemplos a definição de dado pessoal sensível, e o de dado anonimizado, previsto em seu art.5, II e III[12]; e o conceito do que a Lei considera como tratamento de dados, no art. 5, X[13], todos consignados na LGPD.

Aqui cabe observar também sobre o que a norma da LGPD não prevê e o que a concepção de um microssistema jurídico para o ambiente digital em diálogo com outras fontes coerentes e complementares pode auxiliar na exegese mais adequada. O exemplo que segue abaixo ajuda a esclarecer.

Diversamente do que ocorre em relação a outros conceitos inovadores referidos, a LGPD silencia a respeito do que entende por *decisão automatizada* prevista no seu art. 20, §1º[14], que tem por escopo resguardar ao titular de dados o

---

Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais". [...] (grifos nossos).

[11] Lei nº 13.719/18 (LGPD):

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

[12] Art. 5º Para os fins desta Lei, considera-se:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

[13] Art. 5º Para os fins desta Lei, considera-se:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[14] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

direito à revisão quando a *decisão automatizada* afetar seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de *consumo* e de *crédito* ou os aspectos de sua personalidade.

Assim, por exemplo, nas hipóteses de análise de risco envolvendo concessão de crédito[15] para financiamentos e vendas a prazo, a norma estruturante em comento (LGPD) ao prever o direito à revisão não faz referência à legislação específica do Cadastro Positivo que cuida de banco de dados e informações sobre o adimplemento de pessoas naturais ou de pessoas jurídicas, mas faz alusão à legislação consumerista (art. 2º, VI) quando a decisão automatizada[16] se utilizar do *perfil de consumo* do titular de dados e vier a eventualmente a prejudicá-lo.

Como se depreende, ressalta-se que os conceitos destacados na hipótese são complementares (relação de consumo e concessão de crédito) e, por consequência, restam aclarados se analisados em um contexto de integrarem o microssistema jurídico do ambiente digital, uma vez que são normas compatíveis e coerentes entre si, permitindo a consolidação de interpretação doutrinária e jurisprudencial com relação ao seu conteúdo e alcance.

Entrementes, importante referendar que a lei especial (no caso, LGPD) que confere o arcabouço estruturante deve ser apta a promover o tratamento sistêmico a normas afetas ao tema em análise (proteção de dados) que antes se encontrava diluído pelo ordenamento jurídico em diplomas esparsos (*ex. gratia*: Lei de Acesso

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (grifo nosso)

[15] LEI Nº 12.414, DE 9 DE JUNHO DE 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Art. 2º Para os efeitos desta Lei, considera-se:

I - banco de dados: conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro;

[16] Entendemos que se trata do direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

à informação - LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011; Marco Civil da Internet- LEI Nº 12.965, DE 23 DE ABRIL DE 2014; Lei do Cadastro Positivo - LEI Nº 12.414, DE 9 DE JUNHO DE 2011). Bem como, deve ser capaz de superar a divisão entre Direito Público e Privado, Material e Processual, albergando disposições setoriais de todos os ramos do direito.

Com relação a LGPD abarcar normas de direito público, o art. 1º, §único é extreme de dúvidas ao consignar que: "*As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios*". Portanto, todas as Entidades e as esferas descentralizadas da administração pública devem obedecer e conformar sua atuação às disposições contidas nesta lei.

No que tange a abranger normas de direito privado, o artigo 2º, inciso VI[17], da LGPD destaca dentre seus fundamentos o respeito à livre iniciativa e à livre concorrência e a defesa do consumidor; ou seja, os dois primeiros (livre iniciativa e livre concorrência), enquanto primados da reserva de atuação das relações do direito privado, enaltece, respectivamente, o livre exercício da qualquer atividade econômica; e a franca disputa entre as empresas por oportunidades no mercado em condições de igualdade (veda favorecimentos injustificados). E a proteção ao consumidor tem por escopo resguardar parte vulnerável da relação jurídica e reconhecer prerrogativas que favorecem a defesa de direitos.

Concernente à previsão de normas de direito material, voltadas para sopesar quais interesses deverão prevalecer e quais devem ser secundados (uma vez considerados conflitantes), prevê Art. 7, I, que "*O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular*". E é complementado pelo art. 8, §3º, que veda o tratamento de dados

[17] - Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
[...]
VI- a livre iniciativa, a livre concorrência e a defesa do consumidor;

pessoais mediante vício de consentimento. Ou seja, a LGPD adota uma concepção antropocêntrica, que valoriza e procura tutelar a autodeterminação informativa da pessoa natural, titular de dados pessoais, com relação ao tratamento de dados, não tolerando eventual manifestação volitiva viciada, obtido de forma genérica ou precária.

Quanto a comandos processuais, o art. 18, §1º, prevê expressamente que: *"O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional";* que lhe é complementado pelo §8º, que estabelece que: *"O direito a que se refere o §1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor"*. Assim, estão previstos mecanismos instrumentais objetivos e diretos para concretização destas previsões legais em prol do titular de dados ainda em âmbito administrativo.

Não se olvide que no texto da LGPD, além destas disposições legais referidas, outras podem ser pinçadas para complementar os requisitos delineados pela doutrina para caracterizar o microssistema jurídico do ambiente digital.

E quanto a LGPD promover o tratamento sistêmico a normas ligadas ao tema, temos dispositivo de fechamento do ora nominado microssistema jurídico do ambiente digital, que em seu art. 64 apregoa: *"Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte"*.

Acrescente-se a previsão no art. 60 da LGPD, que promoveu alterações legislativas (respectivamente nos arts. 7º e 16 do Marco Civil da Internet (LEI Nº 12.965, DE 23 DE ABRIL DE 2014), remetendo expressamente seus termos para a própria Lei Geral de Proteção de Dados.

Diante do exposto, entende-se que a LGPD preenche os requisitos necessários para funcionar como lei especial estruturante apta a concatenar as

demais normas que cuidam de aspectos da proteção de dados pessoais e se constitui em pedra angular do que ora se denomina de microssistema jurídico do ambiente digital voltado para a proteção da autodeterminação informacional, nos diversos contextos da Sociedade da Informação ou Sociedade de Dados em que estamos imersos.

4 Conclusão

A construção doutrinária e jurisprudencial sobre a proteção de dados pessoais, inclusive no ambiente digital (Lei Nº13.709/2018-LGPD) deve ir ao encontro de estabelecer um diálogo com outras fontes normativas compatíveis como a Lei de Acesso à informação (Lei Nº 12.527/2011), o Marco Civil da Internet (Lei Nº 12.965/2014), a Lei do Cadastro Positivo (Lei nº 12.414/2011) e notadamente a que envolve a proteção de direitos transindividuais (Lei nº 8.078/1990), a fim de interpretar a legislação à luz de vetores coerentes e complementares, conformando-a a realidade e aos direitos fundamentais.

Reconhece-se liame lógico entre o Direito à proteção de dados pessoais e o legislação que cuida dos direitos transindividuais, uma vez que as relações jurídicas constituídas sobre seus ditames apresentam características em comum importantes: risco de sofrer violações com muitas vítimas, com pluralidade de causas e de múltiplos atores, em razão das inúmeras relações telemáticas cotidianas que os cidadãos estão sujeitos; a aplicação do conceito de vulnerabilidade decorrente da assimetria informacional na relação entre os agentes de tratamento de dados (controlador e operador) e o titular dos dados pessoais; bem como a dificuldade de identificar os culpados e delimitar as responsabilidades, exigindo instrumentos jurídicos e entidades especializadas para a proteção coletiva da parte mais fraca.

Restam materializados os requisitos configuradores de um microssistema jurídico do ambiente digital autônomo, voltado para a proteção de dados para além da moldura constitucional (art. 1º, III e 5º, LXXIX, CF/88), uma vez existente lei especial estruturante, consubstanciada na LGPD (Lei nº13.709/18), contendo

princípios básicos novos e específicos como o da autodeterminação informativa e o da adequação, que irradiam seus efeitos para todo o sistema jurídico; e apresenta institutos próprios que lhe garantem características particulares, como o conceito de *dado pessoal sensível* e a definição do que a Lei considera como *tratamento de dados*.

O dinamismo e capacidade de diálogo com outros diplomas normativos compatíveis são considerados requisitos importantes para o microssistema jurídico do ambiente digital, uma vez que deve ser maleável para acompanhar o desenvolvimento tecnológico e integrar novas leis que cuidam de temas relacionados, fortalecendo a segurança jurídica.

A vindoura legislação em discussão em nosso país sobre os usos e aplicações das tecnologias de inteligência artificial deverá se integrar ao microssistema jurídico do ambiente digital, diante da relação de causa e efeitos em envolvendo a coleta e o tratamento de dados pessoais.

7 Referências

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima. A Teoria do Diálogo das Fontes e seu Impacto no Brasil: uma homenagem à Erik Jayme. Revista de Direito do Consumidor, São Paulo, v. 115, ano 27, jan./fev. 2018. Disponível em:https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1042/911. Acesso em: 16 jul. 2023.

CERVO, Fernando António Sacchetim, Codificação, descodificação e recodificação – do monosistema ao polissistema jurídico. Revista Magister de Direito Civil e Processual Civil, 58, 2014. Disponível em: http://www.lex.com.br/doutrina_26099622_CODIFICACAO_DESCODIFICACAO_E_RECODIFICACAO_DO_MONOSSISTEMA_AO_POLISSISTEMA_JURIDICO.aspx, Acesso em 04 jul-2023.

HESSE, Konrad. A força normativa da Constituição. Porto Alegre: Sérgio Antonio Fabris Editor, 1991.

IRTI, Natalino, «L'Etádelladecodificazione» Vent'anni dopo, Milano, Guiffrè, 1998.

JAYME, Erik. Entrevista exclusiva para a Revista Trimestral de Direito Civil - RTDC, dirigida pelo Prof. Dr. Gustavo Tepedino (UERJ), para a seção "Diálogo com a Doutrina", Ed. Padma, Rio de Janeiro, tradução de Claudia Lima Marques. Republicação autorizada. Fonte: Revista Trimestral de Direito Civil, ano 1, vol. 3 jul./ set. 2000, p. 289-293. Disponível em: https://seer.ufrgs.br/ppgdir/article/download/43494/30886. Acesso: 10 out. 2023.

MACEDO, Caio Sperandeo; MALHEIRO, Emerson Penha; CANTON FILHO, Fabio Romeu; FULLER, Greice Patricia; BARRETO JUNIOR, Irineu Francisco; FUJITA, Jorge Shiguemitsu; VIGLIAR, Jose Marcelo Menezes; VÍCOLA, Nivaldo Sebastião; NASPOLINI, Samyra Haydee Dal Farra; JANINI, Tiago Cappi. Microssistema jurídico do ambiente digital [livro eletrônico]. - São Paulo: Ed. dos Autores, 2023. Vários autores. Bibliografia. ISBN 978-65-00-74819-2.

MORAIS, Daniel de Bettencourt Rodrigues Silva. O Direito das Relações privadas dos microssistemas jurídicos: uma perspectiva luso-brasileira (?). REVISTA ESMAT ANO 11 - Nº 18, Pág. 133 - 172 | Edição Especial 2019. Disponível em: http://esmat.tjto.jus.br/publicacoes/index.php/revista_esmat/article/view/307, Acesso em: 17. Jul. 2023.

PENA, Ana Maria Moliterno. Microssistema: o problema do sistema no polissistema. Dissertação apresentada como exigência parcial para obtenção do título de Mestre em Direito, sob a orientação do professor doutor Celso Fernandes Campilongo. São Paulo: Pontifícia Universidade Católica, 2007.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. Disponível site Consultor Jurídico: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-

fundamental#author, Acesso em: 18, Jun. 2023.

STELZER, Joana; GONÇALVES, Everton das Neves; BAPTISTA, Rudá Ryuiti Furukita; VAZ, Rafael Medeiros Popini; WIEIRA, Keite; FIDELIS, Monique de Medeiros. A Lei Geral de Proteção de dados pessoais e os desafios das instituições de ensino superior para a adequação. XIX Colóquio Internacional de Gestão Universitária. Florianópolis, Santa Catarina., Brasil. Nov. 2019, ISBN – 978-85-68618-07-3. Disponível em: https://repositorio.ufsc.br/handle/123456789/201939, Acesso em: 01. Ago. 2023.

SCHREIBER, Anderson; KONDER, Carlos Nelson. Uma agenda para o direito civil-constitucional. Revista Brasileira de Direito Civil – RBDCivil, v. 10, p. 22-23, out./dez. 2016. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/42/36. Acesso em: 11 out. 2023.

TRONCOSO, Christian. RELATÓRIO FINAL - COMISSÃO DE JURISTAS RESPONSÁVEL POR SUBSIDIAR ELABORAÇÃO DE SUBSTITUTIVO SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4. Acesso: 11 out. 2023.

VIEIRA, Marcelo de Mello. Considerações sobre microssistemas jurídicos: definição e importância à luz do direito civil – constitucional brasileiro. Juris Plenum, Ano XVI, nº91, Jan/2020(ISSN-1807-6017). Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2020;1001170488. Acesso em: 22 Jul. 2023.

ZANATTA, Rafael A. F. A tutela coletiva na proteção de dados pessoais. Revista do Advogado, nº144, nov. 2019.

XEXÉO, Leonardo Monteiro. MICROSSISTEMA LEGAL DE TUTELA DAS PESSOAS COM DEFICIÊNCIA. Revista Jurídica Luso Brasileira- RJLB, Ano 4 (2018), nº 4. Disponível em: https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1219_1239.pdf.

Acesso em: 31. Jul. 2023.

ZAVAGLIA COELHO, Alexandre; KLAFKE, Guilherme Forma; MAITO, Deíse Camargo; LATINI, Lucas Maldonado Diz; MARUCA, Giuliana; CHOW, Beatriz Graziano; FEFERBAUM, Marina. Governança da Inteligência Artificial em Organizações: Framework para Comitês de Ética em IA – versão 1.0. São Paulo: CEPI FGV Direito SP, 2023. Disponível em: https://www.bing.com/search?q=arts.+22+e+42%2C+%C2%A7+3&aqs=edge.4.69i64i450l8.1275716422j0j4&FORM=ANAB01&PC=U531. Acesso em: 3 Ago. 2023.

OS DESAFIOS DO MICROSSISTEMA DA LEI GERAL DE PROTEÇÃO DE DADOS À LUZ DOS PRINCÍPIOS CONSTITUCIONAIS BRASILEIROS NA SOCIEDADE DA INFORMAÇÃO

Emerson Penha Malheiro

INTRODUÇÃO

a) Contextualização do microssistema da Lei Geral de Proteção de Dados e a Constituição Federal de 1988 na sociedade da informação

A sociedade contemporânea, caracterizada pela disseminação da tecnologia da informação e pela rápida digitalização de diversos aspectos da vida cotidiana, tem exigido uma reavaliação profunda das relações entre a legislação de proteção de dados e os princípios constitucionais fundamentais.

A Lei Geral de Proteção de Dados (LGPD), instituída no Brasil em 2018, pela Lei n. 13.709/2018, representa uma resposta legislativa à necessidade premente de regulamentação das práticas de tratamento de dados pessoais em consonância com a realidade da sociedade da informação.

A Constituição Federal de 1988, por sua vez, é a carta magna que estabelece os princípios, direitos e garantias fundamentais que orientam a ordem jurídica brasileira.

No contexto da sociedade da informação, diversos desses princípios e direitos consagrados na Constituição, tais como a dignidade da pessoa humana, a privacidade, a liberdade de expressão e a igualdade, assumem uma relevância ainda mais proeminente, dado o impacto que as tecnologias de informação têm sobre a vida das pessoas.

A LGPD, ao criar um microssistema normativo voltado à proteção dos dados pessoais, procura estabelecer diretrizes e normas específicas para a coleta, o tratamento e a utilização desses dados, visando assegurar a privacidade dos indivíduos, bem como o respeito a seus direitos fundamentais.

No entanto, a interação entre esse microssistema legal e os princípios constitucionais é um tema complexo e desafiador.

Inicialmente, a LGPD deve ser interpretada e aplicada à luz dos princípios constitucionais, a fim de assegurar que sua implementação não infrinja ou limite de maneira desproporcional os direitos fundamentais dos cidadãos.

A compatibilidade entre as disposições da LGPD e a Constituição Federal deve ser cuidadosamente examinada, especialmente em casos nos quais os princípios constitucionais entram em conflito com as exigências da legislação de proteção de dados.

Além disso, a sociedade da informação trouxe desafios únicos à proteção de dados pessoais. A coleta massiva e o uso de informações digitais, a inteligência artificial, o comércio eletrônico e a globalização da informação são realidades que demandam uma análise minuciosa sobre como a LGPD pode efetivamente garantir a privacidade e a proteção dos direitos dos indivíduos em um ambiente tão dinâmico e complexo.

Portanto, a contextualização do microssistema da LGPD e da Constituição Federal de 1988 na sociedade da informação é essencial para compreender os desafios e as oportunidades que essa interação apresenta.

A pesquisa e a análise crítica dessa relação são cruciais para garantir que o direito à proteção de dados pessoais seja efetivamente preservado, ao mesmo tempo em que se promove o desenvolvimento tecnológico e a inovação dentro dos limites legais e éticos.

b) Relevância do tema

A relevância do tema "Os Desafios do Microssistema da Lei Geral de Proteção de Dados à Luz dos Princípios Constitucionais Brasileiros na Sociedade da Informação" reside na confluência de dois elementos de importância indiscutível para o ordenamento jurídico e a sociedade contemporânea: a crescente digitalização da informação e a proteção dos direitos fundamentais. Este tópico ganha proeminência à medida que a sociedade da informação se consolida como um fenômeno global, trazendo consigo mudanças substanciais nas formas de coleta, armazenamento, tratamento e compartilhamento de dados pessoais.

A promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil, em 2018, representou um marco legislativo crucial na busca por equilíbrio entre o avanço tecnológico e a preservação dos valores e direitos constitucionais. Nesse contexto, a análise dos desafios enfrentados pelo microssistema da LGPD ao se confrontar com os princípios constitucionais do ordenamento jurídico brasileiro torna-se imperativa.

A proteção de dados pessoais é um dos pilares da privacidade e da liberdade individual, e a LGPD visa assegurar a salvaguarda desse direito fundamental em um ambiente digital complexo e interconectado. A relação entre a LGPD e a Constituição Federal de 1988 é crucial, uma vez que a Carta Magna consagra princípios basilares, como a dignidade da pessoa humana, a intimidade, a vida privada e a liberdade de expressão, que são afetados diretamente pela coleta e uso de dados pessoais.

Além disso, a sociedade da informação trouxe consigo desafios inéditos. A coleta massiva de dados, a inteligência artificial, a internet das coisas e a globalização das comunicações geraram um ambiente no qual a proteção de dados pessoais assume novas complexidades. Portanto, é fundamental analisar como a LGPD, enquanto microssistema normativo, se adapta e responde a esses desafios em consonância com os princípios constitucionais.

A relevância deste tema transcende o âmbito acadêmico, alcançando a esfera prática e política da sociedade. O efetivo equilíbrio entre a proteção de dados

pessoais e a promoção da inovação e do desenvolvimento econômico é um desafio central para a construção de uma sociedade mais justa e igualitária. Portanto, a pesquisa e a análise crítica dos desafios do microssistema da LGPD à luz dos princípios constitucionais contribuem significativamente para a evolução do entendimento jurídico, a tomada de decisões políticas e a salvaguarda dos direitos fundamentais em um mundo digital em constante transformação.

Assim, a relevância deste tema transcende a esfera acadêmica, impactando diretamente a proteção dos direitos dos cidadãos e a construção de uma sociedade que busca conciliar o avanço tecnológico com a preservação dos valores constitucionais fundamentais.

c) Justificativa da escolha do tema

A escolha do tema "Os Desafios do Microssistema da LGPD à Luz dos Princípios Constitucionais Brasileiros na Sociedade da Informação" é fundamentada em uma série de considerações de relevância acadêmica, jurídica e social que justificam sua pertinência e importância.

Em primeiro lugar, vivenciamos uma era marcada pela rápida e abrangente digitalização da sociedade, onde a informação, principalmente os dados pessoais, desempenha um papel central nas interações humanas, na economia e no desenvolvimento tecnológico. Nesse contexto, a promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil representa uma resposta legislativa apropriada e necessária para regulamentar o tratamento de dados pessoais e proteger a privacidade dos cidadãos.

A justificativa para a escolha deste tema também reside no fato de que a proteção de dados pessoais é indissociável dos princípios constitucionais brasileiros. A Constituição Federal de 1988, como a carta magna do país, consagra valores e direitos fundamentais que são diretamente impactados pela coleta e uso de dados

pessoais, tais como a dignidade da pessoa humana, a privacidade, a liberdade de expressão e a igualdade.

Além disso, a dinâmica da sociedade da informação apresenta desafios e complexidades únicos para a proteção de dados pessoais. A coleta massiva de informações, o poder dos algoritmos, a interconexão global e a proliferação de dispositivos conectados geram questões jurídicas complexas que devem ser abordadas em consonância com os princípios constitucionais.

Nesse contexto, a justificativa para a escolha deste tema reside na necessidade premente de uma análise crítica e aprofundada da interação entre a LGPD e a Constituição Federal, visando identificar as tensões, os desafios e as oportunidades que essa relação oferece. A pesquisa sobre os desafios do microssistema da LGPD à luz dos princípios constitucionais brasileiros tem a capacidade de enriquecer o entendimento jurídico, fornecer orientações práticas para a aplicação da legislação e contribuir para o desenvolvimento de políticas públicas que assegurem a proteção dos direitos fundamentais dos cidadãos em um ambiente digital em constante evolução.

Portanto, a escolha deste tema representa um esforço acadêmico e intelectual para iluminar os caminhos pelos quais a proteção de dados pessoais e os princípios constitucionais podem coexistir harmoniosamente na sociedade da informação, garantindo, assim, a efetiva preservação da dignidade, liberdade e privacidade dos indivíduos em um mundo cada vez mais interconectado e orientado pela informação.

1. Princípios constitucionais e a sociedade da informação

1.1 Princípios constitucionais relevantes e sua conexão com a sociedade da informação

No âmbito do Direito Constitucional brasileiro, diversos princípios fundamentais desempenham um papel crucial na conexão com a sociedade da informação, onde a tecnologia e a informação digital desempenham um papel central.

Esses princípios orientam a interpretação e a aplicação das normas constitucionais em um contexto de rápida transformação tecnológica e de digitalização.

No entanto, é importante lembrar que os princípios estabelecem direitos que são inseparáveis dos seus respectivos deveres, tanto no Brasil quanto no exterior, afinal, "A bem da verdade, cabe proclamar que o obscurantismo da indissolubilidade dos vínculos entre direitos e deveres não se acha adstrito ao Brasil, tratando-se de fenômeno presente na sociedade industrial avançada" (FIORILLO, 2015, p. 33).

Destacam-se alguns dos princípios mais relevantes nessa conexão:

a) Dignidade da pessoa humana: cuida-se de um dos pilares fundamentais da Constituição de 1988. Na sociedade da informação, este princípio reforça a importância de proteger a autonomia e a integridade dos indivíduos em um ambiente digital. A coleta massiva de dados e a utilização de tecnologias avançadas exigem medidas para garantir que a dignidade das pessoas não seja violada por meio do uso indevido de suas informações pessoais. "A proteção da dignidade da pessoa humana envolve todos os aspectos do indivíduo, sem exceção" (MALHEIRO, 2016a, p. 29).

b) Privacidade: o direito à privacidade, consagrado no artigo 5º, inciso X, da Constituição, é especialmente relevante na sociedade da informação. "Toma-se, pois, a privacidade como o conjunto de informação acerca do indivíduo que ele pode decidir manter sobre seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso ser legalmente sujeito" (SILVA, 2022, p. 208). A proteção da privacidade envolve o controle sobre os dados pessoais e a

preservação da intimidade dos cidadãos em um contexto onde as informações pessoais são coletadas e compartilhadas em larga escala.

c) Liberdade de expressão e informação: os princípios da liberdade de expressão e informação, previstos no artigo 5º, incisos IV e XIV, têm um papel fundamental na sociedade da informação, onde a troca de informações e a liberdade de comunicação são valorizadas. No entanto, é necessário equilibrar esses princípios com a proteção de dados pessoais para evitar abusos e preservar o direito à privacidade, mesmo porque "A liberdade de expressão encontra limites previstos diretamente pelo constituinte como também descobertos pela colisão desse direito com outros de mesmo *status*" (MENDES; BRANCO, 2015, p. 270).

d) Igualdade: o princípio da igualdade, previsto no caput do artigo 5º da Constituição, também é relevante na sociedade da informação, pois visa garantir que todos os cidadãos tenham igualdade de acesso às oportunidades e benefícios proporcionados pela tecnologia e pela informação digital, evitando a criação de disparidades injustas. É importante salientar que "Não existe um direito à igualdade em abstrato, mas uma pessoa é igual em algo e em relação a outra pessoa"[18] (PÉREZ et al.2016, p. 606).

e) Devido processo legal: o devido processo legal, previsto no inciso LIV do artigo 5º, assegura que os direitos das pessoas sejam protegidos de acordo com as garantias processuais adequadas, inclusive no contexto digital. Isso é fundamental para garantir que os cidadãos tenham meios eficazes de contestar decisões que afetem seus direitos na era digital.

f) Acesso à justiça: o acesso à justiça, um princípio fundamental, implica que os cidadãos devem ter meios acessíveis e eficazes para buscar reparação em caso de violação de seus direitos na sociedade da informação. Isso inclui questões relacionadas à proteção de dados pessoais.

[18] Tradução livre de: "No existe um derecho a la igualdad em abstracto, sino que se es igual em algo y respecto de alguien."

g) Legalidade e reserva legal: os princípios da legalidade e reserva legal exigem que as restrições aos direitos e liberdades individuais sejam estabelecidas por leis claras e específicas. No contexto da proteção de dados, isso implica que as normas que regem a coleta, o tratamento e o compartilhamento de informações pessoais devem ser bem definidas e previsíveis.

h) Transparência e responsabilização: embora não sejam princípios constitucionais explícitos, a transparência e a responsabilização são fundamentais na sociedade da informação. Esses princípios exigem que as organizações e autoridades que lidam com dados pessoais sejam transparentes em relação às suas práticas e sejam responsáveis por qualquer uso indevido ou inadequado desses dados. Todavia, não se pode ignorar que "O problema surge a partir da dificuldade que os meios eletrônicos trazem no que se refere à busca da responsabilização do agente causador dos danos" (TEIXEIRA, 2015, p. 261).

A Constituição Federal de 1988 estabelece um conjunto sólido de princípios que têm relevância direta na sociedade da informação, fornecendo a base para a interpretação e aplicação das leis de proteção de dados e garantindo que os direitos e liberdades individuais sejam preservados em um ambiente digital em constante evolução. Esses princípios orientam a legislação, a jurisprudência e as políticas públicas relacionadas à proteção de dados pessoais no Brasil.

1.2 A sociedade da informação e a proteção de dados

A sociedade da informação representa uma era marcada por avanços tecnológicos sem precedentes, nos quais a informação e a comunicação desempenham papéis centrais em todos os aspectos da vida humana.

> A sociedade da informação é uma nova representação de composição da coletividade social, que se estabelece em uma forma de evolução em que a informação, como elemento primordial para conceber conhecimento, representa uma atribuição essencial na geração de afluência material e na contribuição para a satisfação e qualidade de vida das pessoas (MALHEIRO, 2016b, p. 17).

Nesse contexto, a interpretação e aplicação dos princípios constitucionais relacionados à proteção de dados pessoais enfrentam desafios significativos que requerem uma análise cuidadosa e uma abordagem adaptativa por parte dos intérpretes e aplicadores do Direito.

Os princípios constitucionais, em particular aqueles relacionados aos direitos fundamentais, são indispensáveis para a garantia dos direitos e liberdades dos cidadãos em uma sociedade democrática.

No entanto, a sociedade da informação trouxe consigo uma explosão na coleta, processamento e compartilhamento de dados pessoais, muitas vezes sem o pleno conhecimento ou consentimento dos titulares desses dados.

Isso cria tensões significativas entre a necessidade de proteger a privacidade e a liberdade individual e a necessidade de facilitar o fluxo de informações e o desenvolvimento tecnológico.

Um dos desafios mais prementes é a necessidade de reinterpretar os princípios constitucionais à luz das novas realidades da sociedade da informação.

A interpretação tradicional desses princípios pode não ser adequada para lidar com questões complexas, como a retenção indefinida de dados, a análise de big data e a vigilância em massa.

Portanto, os intérpretes do Direito devem adotar uma abordagem dinâmica e evolutiva, buscando harmonizar os princípios constitucionais com os avanços tecnológicos e as novas ameaças à privacidade.

Além disso, a aplicação eficaz dos princípios constitucionais no contexto da proteção de dados pessoais requer a criação e atualização de leis e regulamentações que sejam relevantes e proporcionais aos desafios específicos da sociedade da informação.

Isso envolve a elaboração de legislação que promova a transparência, o consentimento informado e a responsabilidade das organizações que coletam e processam dados pessoais.

Também é necessário estabelecer mecanismos de supervisão e fiscalização eficazes para garantir o cumprimento dessas leis.

Outro aspecto importante é a cooperação internacional na proteção de dados pessoais, uma vez que os dados muitas vezes atravessam fronteiras.

Os princípios constitucionais devem ser aplicados de maneira consistente e coordenada em nível global, por meio de acordos e tratados internacionais, para evitar lacunas na proteção dos direitos individuais.

A sociedade da informação apresenta desafios significativos para a interpretação e aplicação dos princípios constitucionais no contexto da proteção de dados pessoais.

> Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação (BIONI, 2021, p. 12).

A adaptação do Direito às novas realidades tecnológicas requer uma abordagem flexível, legislação atualizada e cooperação internacional.

A proteção efetiva da privacidade e dos direitos individuais é fundamental para garantir que a sociedade da informação continue a ser uma força positiva para o desenvolvimento humano e o progresso social.

2. A LGPD como microssistema normativo

A crescente digitalização da sociedade e a massiva coleta e tratamento de dados pessoais trouxeram à tona a necessidade premente de regulamentar a proteção desses dados.

A proteção de dados pessoais é disciplinada pela Lei n. 13.709/2018, com a redação conferida pela Lei n. 13.853/2019, que alterou vários artigos daquela lei,

incluindo a ementa que passou a ter a seguinte redação: "Lei Geral de Proteção de Dados (LGPD)".

A LGPD, inspirada em marcos legais como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), é uma legislação abrangente que estabelece diretrizes para o tratamento de dados pessoais no Brasil.

"Dada a relevância que os dados pessoais têm na sociedade da informação, é de extrema importância ter uma lei que estabeleça normas gerais para sua proteção" (SALES, 2021, p.19)

No entanto, sua relevância transcende sua mera função regulatória; a LGPD pode ser considerada um microssistema normativo, pois engloba um conjunto de regras interconectadas que regem um campo específico do Direito.

2.1 Características da LGPD como microssistema normativo

São características da LGPD como microssistema normativo:

a) Abordagem abrangente: a LGPD não se limita a definir apenas princípios gerais, mas também incorpora disposições detalhadas que regulam a coleta, processamento e compartilhamento de dados pessoais. Ela cria uma estrutura jurídica completa para a proteção de dados, incluindo definições específicas, obrigações para controladores e operadores de dados, direitos dos titulares e mecanismos de fiscalização.

b) Princípios fundamentais: a LGPD estabelece princípios fundamentais, como o princípio da finalidade, da necessidade, da transparência e da responsabilização, que norteiam todas as suas disposições. Esses princípios refletem a importância de se equilibrar a proteção dos direitos dos titulares com a necessidade de processar dados pessoais para fins legítimos.

c) Interconexões com outros ramos do Direito: a LGPD não atua isoladamente. Ela se conecta com outras áreas do Direito, como o Direito do Consumidor, o Direito Civil, o Direito Penal e o Direito Administrativo. Isso ocorre

porque a proteção de dados pessoais afeta diversas relações jurídicas, como contratos, responsabilidade civil e investigações criminais.

d) Órgãos reguladores e fiscalizatórios: a LGPD cria a Autoridade Nacional de Proteção de Dados (ANPD) como o órgão responsável por supervisionar e fiscalizar o cumprimento da lei. Essa autoridade desempenha um papel crucial na aplicação efetiva da LGPD e na solução de controvérsias.

2.2 Diretrizes estruturais da LGPD como microssistema normativo

A LGPD não é apenas um marco normativo. Ela representa um paradigma legal que influencia significativamente as interações entre indivíduos, organizações e o Estado na era da informação digital.

Ao promover a proteção da privacidade e dos direitos individuais, a LGPD fomenta a confiança pública no uso de serviços online e estimula a inovação responsável.

Além disso, a legislação coloca o Brasil em conformidade com padrões internacionais de proteção de dados, facilitando o fluxo transfronteiriço de informações.

A LGPD estabelece uma estrutura sólida para a proteção de dados pessoais, incorporando diretrizes estruturais essenciais:

a) Titulares de dados: a LGPD concede aos titulares dos dados uma série de direitos, incluindo o acesso aos dados, a correção de informações imprecisas, a exclusão de dados desnecessários e a portabilidade de dados. "O titular de dados, portanto, é a pessoa que vai receber a proteção conferida pela LGPD,vale dizer, em última análise, é a destinatária da lei em questão e a quem são conferidos os direitos dela decorrentes" (SALES, 2021, p. 65). Esses direitos fortalecem o controle individual sobre as informações pessoais.

b) Controladores e operadores: a lei distingue claramente as funções e responsabilidades dos controladores e operadores de dados. Essa distinção

promove uma clara atribuição de responsabilidade e papel na gestão dos dados pessoais.

c) Sanções e fiscalização: a LGPD prevê sanções substanciais para o não cumprimento das normas, demonstrando o compromisso com a aplicação rigorosa da lei. A Autoridade Nacional de Proteção de Dados (ANPD) exerce um papel de destaque na supervisão e fiscalização.

2.3 Desafios na implementação da LGPD como microssistema normativo à luz dos princípios constitucionais

A aplicação da Lei Geral de Proteção de Dados (LGPD) como microssistema normativo à luz dos princípios constitucionais enfrenta diversos desafios práticos, que podem ser analisados em várias dimensões.

É importante identificar esses desafios para promover uma análise crítica e propositiva.

A seguir, alguns dos principais desafios:

a) Equilíbrio entre privacidade e interesses legítimos: um dos princípios fundamentais da LGPD é a proteção da privacidade, conforme garantido na Constituição. No entanto, a aplicação da lei também deve levar em consideração os legítimos interesses das empresas e do Estado, como a segurança pública e o desenvolvimento econômico. O desafio está em encontrar um equilíbrio adequado entre a proteção da privacidade e a promoção desses interesses, respeitando os princípios constitucionais da proporcionalidade e da razoabilidade.

b) Adequação à realidade tecnológica: "O avanço tecnológico na comunicação sempre perseguiu o objetivo de criar uma Aldeia Global, permitindo que todas as pessoas do mundo pudessem ter acesso a um fato de modo simultâneo" (PINHEIRO, 2016, p. 67). A rápida evolução tecnológica apresenta um desafio constante para a aplicação da LGPD. Novas tecnologias, como a inteligência artificial e a Internet das Coisas, levantam questões complexas sobre como os dados

pessoais são coletados e processados. Garantir que a LGPD permaneça relevante e eficaz diante dessas inovações é uma tarefa desafiadora.

c) Conscientização e educação: a eficácia da LGPD depende da conscientização e do entendimento por parte dos titulares de dados, das empresas e das instituições públicas. A educação sobre direitos de privacidade e responsabilidades em relação à proteção de dados é fundamental. Os desafios incluem a disseminação eficaz de informações sobre a LGPD e a promoção da cultura de proteção de dados na sociedade.

d) Cooperação internacional: em um mundo globalizado, muitos dados pessoais cruzam fronteiras. A LGPD estabelece regras para a transferência internacional de dados, mas a harmonização das leis de proteção de dados entre países é um desafio. Garantir que os princípios da LGPD sejam respeitados em contextos internacionais requer cooperação e acordos com outras jurisdições.

e) Capacidade de fiscalização e aplicação: a fiscalização e a aplicação da LGPD são cruciais para garantir sua eficácia. A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central nesse processo. No entanto, a ANPD enfrenta desafios relacionados a recursos, pessoal e infraestrutura para lidar com o grande volume de casos e garantir o cumprimento da lei de maneira consistente.

f) Complexidade da interconexão de normas: a LGPD interage com outros ramos do Direito, como o Direito do Consumidor, o Direito Contratual e o Direito Penal. A complexidade dessa interconexão cria desafios na aplicação consistente da lei e na interpretação de suas implicações em diferentes contextos jurídicos.

g) Responsabilidade corporativa: as empresas precisam se adaptar para cumprir as obrigações da LGPD, o que pode ser especialmente desafiador para pequenas e médias empresas. Garantir que as empresas de todos os tamanhos estejam em conformidade é um desafio prático, que envolve educação, recursos financeiros e capacidade técnica.

A aplicação da LGPD como microssistema normativo à luz dos princípios constitucionais enfrenta desafios práticos significativos.

Esses desafios requerem uma abordagem multidisciplinar e contínua, envolvendo o governo, a sociedade civil, as empresas e as instituições acadêmicas.

A busca por soluções eficazes é crucial para garantir a proteção efetiva dos direitos de privacidade dos cidadãos na sociedade da informação.

3. Desafios e soluções na harmonização da LGPD com a Constituição Federal de 1988

Discute-se os desafios específicos que surgem ao tentar harmonizar a LGPD com os princípios constitucionais e são oferecidas possíveis soluções ou recomendações.

3.1 Tensões e conflitos entre a LGPD e a Constituição Federal de 1988

As tensões entre a LGPD e a Constituição Federal emergem principalmente no que diz respeito à harmonização da proteção da privacidade e à garantia da livre iniciativa e da livre expressão. Alguns dos pontos de conflito incluem:

a) Limitações à liberdade de expressão: a LGPD impõe restrições à coleta e ao tratamento de dados pessoais, o que pode colidir com a liberdade de expressão, especialmente em ambientes online, onde a análise de dados é essencial para a personalização de conteúdo.

b) Direitos fundamentais e interesses econômicos: a LGPD busca proteger os direitos fundamentais à privacidade e à proteção de dados, muitas vezes em detrimento de interesses econômicos, uma vez que impõe regras rigorosas às empresas que coletam e tratam dados pessoais.

c) Necessidade de regulamentação específica: a Constituição Federal estabeleceu os princípios gerais da proteção de dados, mas a LGPD detalha as

obrigações e responsabilidades em relação à proteção de dados pessoais. Isso pode gerar dúvidas sobre como conciliar essas duas fontes normativas.

3.2 Soluções para a harmonização da LGPD com a Constituição Federal de 1988

A abordagem para resolver essas tensões e conflitos entre a LGPD e a Constituição Federal deve ser pautada na interpretação harmonizadora, respeitando-se a primazia dos direitos fundamentais.

É fundamental que os operadores do direito e os tribunais considerem a necessidade de um equilíbrio entre a proteção da privacidade e os interesses legítimos da sociedade e das empresas.

Nesse sentido, a jurisprudência e a doutrina desempenham um papel vital na definição de como esses dois pilares do ordenamento jurídico brasileiro podem coexistir de forma coesa e eficaz.

É imperativo que a análise de casos concretos leve em consideração os princípios da proporcionalidade e da razoabilidade, bem como o respeito à dignidade humana e à autonomia do indivíduo.

As tensões e conflitos entre a LGPD e a Constituição Federal de 1988 são uma realidade intrínseca ao ambiente jurídico da sociedade da informação.

É uma tarefa constante dos juristas e acadêmicos encontrar soluções que assegurem a proteção da privacidade dos cidadãos sem comprometer as liberdades individuais e a inovação. Essa discussão e busca por equilíbrio são cruciais para o avanço do Direito da Sociedade da Informação em nosso país.

No contexto da complexa relação entre a Lei Geral de Proteção de Dados (LGPD) e a Constituição Federal de 1988, é imperativo buscar soluções que permitam a harmonização dessas duas fontes normativas, preservando a proteção da privacidade e os direitos fundamentais dos cidadãos, ao mesmo tempo em que se promove o desenvolvimento econômico e tecnológico.

Abaixo, apresento algumas soluções que podem contribuir para essa harmonização:

a) Princípio da proporcionalidade e razoabilidade: Utilizar o princípio da proporcionalidade e razoabilidade como norte na interpretação e aplicação da LGPD. Isso significa que qualquer restrição aos direitos fundamentais deve ser estritamente necessária para atingir um objetivo legítimo e deve ser apropriada ao contexto.

b) Interpretação sistemática: Realizar uma interpretação sistemática da LGPD em relação à Constituição Federal, considerando os princípios constitucionais que regem a proteção de dados pessoais, como a inviolabilidade da intimidade e da vida privada.

c) Legislação setorial: Elaborar legislação setorial que aborde especificamente áreas em que a LGPD e a Constituição Federal colidem, como a liberdade de expressão na internet e a pesquisa científica. Essas leis podem estabelecer diretrizes mais precisas para equilibrar os interesses em jogo.

d) Educação e conscientização: Promover a educação e a conscientização sobre proteção de dados e privacidade tanto para os cidadãos quanto para as empresas. O conhecimento sobre os direitos e responsabilidades sob a LGPD pode ajudar a prevenir conflitos.

e) Órgãos reguladores e fiscalização: Reforçar os órgãos reguladores e mecanismos de fiscalização da LGPD para garantir que as empresas cumpram suas obrigações de proteção de dados, mas também para evitar abusos na aplicação da lei.

f) Jurisprudência consolidada: Estabelecer uma jurisprudência consolidada sobre questões de privacidade e proteção de dados, de modo a criar precedentes que orientem casos futuros e garantam a consistência na aplicação da lei.

g) Diálogo multissetorial: Promover um diálogo constante e construtivo entre os setores público, privado e a sociedade civil para discutir questões relacionadas à proteção de dados e à sua harmonização com a Constituição.

h) Revisão e atualização: Revisar e atualizar a LGPD conforme necessário, levando em consideração as mudanças tecnológicas e sociais que afetam a privacidade e a proteção de dados.

i) Transparência e responsabilidade: Incentivar as empresas a adotar políticas de transparência e responsabilidade em relação à coleta e tratamento de dados pessoais, fornecendo aos usuários maior controle sobre suas informações.

j) Mediação e arbitragem: Promover mecanismos alternativos de resolução de conflitos, como mediação e arbitragem, para resolver disputas relacionadas à proteção de dados de forma eficiente e menos adversarial.

A harmonização da LGPD com a Constituição Federal requer uma abordagem equilibrada que respeite os direitos fundamentais dos cidadãos e promova o desenvolvimento tecnológico e econômico.

A busca por soluções deve ser contínua, envolvendo todos os setores da sociedade e adaptando-se às mudanças dinâmicas no cenário da sociedade da informação.

CONCLUSÃO

No contexto da crescente importância da proteção de dados pessoais na sociedade da informação, a promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil representou um avanço significativo na regulamentação desse campo. O microssistema da LGPD trouxe consigo inúmeros desafios que exigem uma análise cuidadosa sob a perspectiva dos princípios constitucionais brasileiros.

Ao longo deste artigo jurídico-científico, examinamos esses desafios e destacamos a necessidade de encontrar um equilíbrio delicado entre a proteção da privacidade e a promoção do desenvolvimento tecnológico e econômico. A conciliação desses objetivos não é tarefa simples, uma vez que a LGPD, embora crucial para salvaguardar direitos fundamentais, também pode impactar a livre iniciativa, a inovação e a liberdade de expressão.

Diante desse cenário, é imperativo que o sistema jurídico brasileiro continue a evoluir, levando em consideração as características únicas da sociedade da informação. Os princípios constitucionais, como a dignidade da pessoa humana, a inviolabilidade da intimidade e da vida privada, devem guiar a interpretação e aplicação da LGPD, assegurando que os direitos individuais sejam protegidos sem sufocar a inovação e o progresso tecnológico.

Nesse sentido, é fundamental que juristas, legisladores, operadores do direito e demais atores da sociedade estejam envolvidos em debates e discussões construtivas para encontrar soluções que permitam a harmonização da LGPD com os princípios constitucionais brasileiros. Essa busca contínua por equilíbrio e adaptação às mudanças na sociedade da informação é essencial para garantir que a proteção de dados pessoais seja eficaz e compatível com as demandas do mundo digital.

Em última análise, os desafios apresentados pelo microssistema da LGPD são reflexo do dinamismo e da complexidade da sociedade contemporânea. A capacidade de enfrentar esses desafios de maneira ética e legalmente sólida será determinante para o sucesso da legislação de proteção de dados pessoais no Brasil, assegurando que os direitos individuais e coletivos sejam respeitados em um ambiente digital em constante evolução.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. São Paulo: Forense, 2021.

FIORILLO, Celso Antonio Pacheco. Princípios constitucionais do direito da sociedade da informação: a tutela jurídica do meio ambiente digital. São Paulo: Saraiva, 2015.

MALHEIRO, Emerson Penha. Curso de direitos humanos. 3. ed. São Paulo: Atlas, 2016a.

MALHEIRO, Emerson Penha. Direito da sociedade da informação. São Paulo: Max Limonad, 2016b.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Bonet. Curso de direito constitucional. 10. ed. São Paulo: Saraiva, 2015.

PÉREZ, Miguel A. Aparicio; SERRAMALERA, Mercè Barceló i. Manual de derecho constitucional. 3. ed. Barcelona: Atelier Libros Jurídicos, 2016.

PINHEIRO, Patricia Peck. Direito digital. 6. ed. São Paulo: Saraiva, 2016.

SALES, Fernando Augusto de Vita Borges de. Manual da LGPD. Leme: Mizuno, 2021.

SILVA, José Afonso da. Curso de direito constitucional positivo. 44. ed. São Paulo: 2022.

TEIXEIRA, Tarcísio. Curso de direito e processo eletrônico. 3. ed. São Paulo: Saraiva, 2015.

VANTAGENS DO MICROSSISTEMA JURÍDICO

Fabio Romeo Canton

O microssistema jurídico surge a partir de temas que demandam tratamento diferenciado pelo legislador, seja pela sua abrangência, seja por sua especificidade. É o que já se verificou, a título de exemplo, com as relações de consumo, com a criança e o adolescente e mais recentemente com a proteção de dados e a inteligência artificial.

As relações humanas são dinâmicas e permanentemente experimentam novos contornos e demandas. A sociedade da informação é pródiga em propiciar mudanças de eixo com a apresentação de demandas inéditas que exigem tratamento diferenciado e específico. Na sociedade da informação os dados assumem especial relevo, não apenas na disseminação da informação direta, mas também e especial ente como elemento construtor de acervos cognitivos de instrução e orientação, pessoal e de mercado, imantados e trabalhados à exaustão como base de construção de novos paradigmas e mesmo realidades, inclusive paralelas e eventualmente incontroláveis, como a inteligência artificial.

A atenção dispensada no tratamento jurídico de determinadas matérias, faz surgir, intencionalmente ou não, um microssistema jurídico, portador de normas materiais e formais mais adequadas ao objeto de destino. A primeira vantagem exsurge exatamente da atenção dedicada a determinado tema. Antes mesmo de eventual processo legislativo, como fruto da dinâmica social, novos fenômenos que permeiam as relações humanas passam a despertar mais interesse e atenção e,

consequentemente, mais preocupação, mais dúvidas, mais indagações, e uma natural percepção da necessidade de tratamento jurídico próprio, do que se extrairá um aprofundamento no estudo de suas ocorrências e implicações, positivas e negativas.

A atenção natural ou provocada, portanto, propiciará que mais pessoas se debrucem sobre o tema de forma mais aprofundada, facilitando perspectivas empíricas e teóricas que servirão de esteio para a construção de um sistema jurídico de tratamento mais adequado.

O microssistema, assim, tende a surgira surgir mais consolidado desde o início com relação ao tema de que trata, pois que precedido de análise específica e mais profunda.

O processo legislativo de criação do microssistema também refletira essa qualidade, pois despertará o interesse de especialistas. Ou seja, não apenas o legislador voltado a determinada matéria terá melhores condições de compreender as demandas relativas a ela, como todo o caminho será auxiliado por especialista, do que resultará um notório ganho de qualidade na elaboração do projeto legislativo.

A criação da lei em si, de outro lado, também representa uma vantagem. Diversamente da codificação que tem sob foco uma gama enorme de temas, a lei específica, monotemática, evita uma natural dispersão de atenção, além evitar um incontável número de impasses das mais variadas ordens, tendo em vista a multiplicidade de assuntos que as codificações ostentam e tratam em seu conteúdo.

Notória vantagem, e talvez a principal, também decorre do conteúdo do microssistema. Vocacionado à matéria específica permite, como resultado de maior e melhor análise prévia, a construção de um conteúdo de maior qualidade e apto a atender melhor e de forma mais eficiente e mais rápida as situações concretas a reclamar tutela legislativa própria.

Não só isso. Permite o microssistema, para além e de forma diversa da codificação clássica, a elaboração, em uma única estrutura, de normas de cunho

material e normas de cunho processual, sob um enfoque específico e mais adequado.

Além disso, é preciso considerar o tempo médio para a aprovação de estruturas legislativas complexas como as codificações a demandar, não raras vezes, décadas. O Código Civil é um eloquente exemplo da demora do processo legislativo para aprovação de um código. Nesse aspecto, é comum dizer que algumas leis já nascem desatualizadas, tendo em vista o longo lapso temporal decorrido entre a sua idealização e a sua aprovação.

No âmbito do microssistema, portanto, o jurisdicionado, destinatário final das normas, tem a seu dispor um instrumento legislativo mais adequado, moderno e atual, pois contemporâneo às relações jurídicas que se pretende regular. Na estrutura codificada, diversamente, conforme já se apontou, algumas relações complexas, que reclamavam tratamento legal, talvez nem existam mais quando da aprovação do código respectivo.

Sendo a vida em sociedade e as relações humanas dinâmicas, em constante mudança, é relevante imaginar que uma estrutura legislativa mais simples ofereça a vantagem de permitir alterações muito mais rápidas. A velocidade das mudanças na sociedade da informação dá uma boa medida da necessidade social do ponto de vista temporal no que respeita à criação e à modificação de leis.

O microssistema permite driblar as sempre presentes resistências para a criação e alteração de códigos, pois o fenômeno normalmente não se verídica fora dessa estrutura complexa.

Mudanças sociais, portanto, que demandem alterações legislativas de um microssistema, podem mais rápida e eficientemente ser atendidas, pois que o processo legislativo é mais simples, não só pela sua forma, mas também porque o seu conteúdo, não tão abrangente como o de um código, afasta usuais resistências, além de permitir, conforme o caso concreto, a criação de normas de direito material,

acompanhada de norma processual respectiva que será utilizada para encaminhar e materializar o direito previsto.

A tutela que o legislador pretende, portanto, como reflexo da vontade do cidadão em face de relações jurídicas e sociais específicas, pode muito mais facilmente, em tempo adequado, ser atendida.

Essa é uma ligeira e breve exposição de reflexões acerca do microssistema e as vantagens que pode oferecer ao sistema jurídico e à sociedade como um todo.

O MICROSSISTEMA JURÍDICO DO AMBIENTE DIGITAL NA TUTELA PENAL

Greice Patrícia Fuller

Introdução

O artigo tem por objetivo analisar tema inédito na esfera penal nacional sobre o microssistema jurídico do ambiente digital, observando-se a necessidade de uma nova construção dogmática, interdisciplinar, sistemática, compreendendo aspectos específicos em relação aos destinatários, objeto de tutela e base principiologia.

Trata-se de artigo que inicia informando as características inerentes à criminalidade na sociedade da informação, subsumindo, em momento posterior a ideia de ambiência digital no contexto do meio ambiente cultural e, ao final, propugnando, por meio do diálogo entre fontes normativas interdisciplinares, o denominado microssistema jurídico penal do ambiente digital. Para tal construção doutrinária, propõe-se a construção de um microssistema jurídico-penal (condensando normas de direito material e processual) que deve ser estruturado a partir da análise sobre os bens jurídicos relevantes ao Direito Penal. Assim, parte-se do pressuposto de que o meio ambiente digital apresenta bens jurídico-penais coletivos *lato sensu*, próprios, indicando a Constituição Federal e a Lei nº 13.709, de 14 de agosto de 2018 conhecida como Lei Geral de Proteção de Dados (LGPD) como fundamentais à reflexão temática, visto que apresenta como tutela a proteção de dados, bem como, segurança informacional.

A metodologia utilizada foi a lógico-dedutiva, utilizando-se de pesquisa bibliográfica de cunho nacional e internacional.

1. Aspectos propedêuticos sobre a criminalidade na sociedade da informação: novo paradigma fático e jurídico no século XXI

O conceito de sociedade da informação aparece no cenário da revolução tecnológica propiciada no fim do século XIX depois da Segunda Guerra Mundial e geradora da modificação das estruturas sociais, culturais, econômicas e políticas e da geração do amplo acesso à informação, desenvolvendo novos modelos organizacionais assim como novos mercados socioeconômicos.

Nesse ponto, faz-se clara a ideia de que a sociedade da informação sob a vertente de Takeo Takashi, "não é um modismo (...) Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um novo paradigma técnico-econômico".

No dizer de Habermas sobre o assunto, nota-se que :

> Entrementes, as sociedades pós-industriais são caracterizadas por um setor quaternário de trabalho baseado no saber – como as indústrias high-tech ou os serviços de saúde, os bancos ou a administração pública -, que depende da afluência de novas informações e, em última análise, de pesquisa e inovação (HABERMAS, 2001).

Portanto, a sociedade da informação apresenta características pontuais por ter a potencialidade de ser instrumento tendente à inclusão digital, especialmente por meio da educação, propiciar o intercâmbio de informações e comunicações de maneira célere e transnacional, dissolver as fronteiras comunicacionais de massa e ter o seu uso como um fator geração econômica diante do ciclo civilizatório atual, dentre outros aspectos de cunho positivo ao Estado Democrático de Direito e à efetividade do princípio da dignidade da pessoa humana.

Contudo, o uso das novas tecnologias pode gerar atos ilícitos e caracterizadores de violência.

Segundo Jesús Ballesteros (2006, p. 16), violência pode ser assim entendida:

> Tanto la etimología como el uso ordinario de la palabra violencia implican la negación del respeto debido a una persona o a una regla. Así el verbo latino violo, del que procede, significa maltratar, ultrajar, deshonrar o profanar, es decir, lo contrario del verbo parco, que equivale a respetar, cuidar, perdonar. En el lenguaje ordinario, violar a una persona, una ley o un contrato indica igualmente esta idea de omisión del respeto exigido Esta negación del respeto distingue la realidad de la violencia del simple empleo de la fuerza, que obliga a otra persona a hacer lo que no desearía, ya que este empleo de la fuerza puede estar en cambio legitimado por razones de defensa de la paz, o por conveniencia de la propia persona coaccionada.

Hannah Arendt seguindo a linha de pensamento de Engels afirma que a violência necessita ferramentas. E, a revolução tecnológica que pressupõe a sociedade da informação, inegavelmente considera-se uma das ferramentas da violência[19].

Nesse contexto, conclui-se que com o seu avanço, as condutas praticadas por meio das novas tecnologias acabam por violar bens jurídicos estabelecidos constitucionalmente ganhando novos delineamentos geradores de perenidade quanto aos seus resultados no espaço virtual.

Eloy Velasco Nuñez (2006, p. 123) afirma que há duas classes de delitos informáticos, quais sejam: a) delitos tipificados na parte geral do Código Penal, mas cometidos através de meios informáticos, como *v.g.* estelionato e ameaça cometidos através de internet; b) delitos específicos informáticos como *cracking* ou sabotagem, *hacking,* proteção de software etc

[19] Slavoj Zizek afirma que há três aspectos de violência, a saber: a subjetiva que inclui a simbólica e a sistêmica decorrentes do funcionamento irregular dos sistemas econômicos e políticos.In: ZIZEK, Slavoj. **Violência: seis reflexões laterais.** São Paulo: Biotempo, 2014, p. 17.

No cenário da criminalidade informática, surgem tipos penais com características específicas de celeridade em sua consecução, gerando consequências e resultados em menor tempo e em maior extensão no ciberespaço; variabilidade em seu *modus operandi*; anonimato; facilidade na realização, tendo em vista não exigir dispêndio econômico; possibilidade de desvio e dilapidação de contexto probatório; atingimento de um número indeterminado de vítimas (em alguns casos, como *v.g*. ciberterrorismo) ou determinável de vítimas em delitos, *v.g*. de crimes patrimoniais ou invasões de dispositivos informáticos; perenidade dos resultados (*v.g*. crimes praticados contra a honra em redes sociais).

Segundo Greice Patrícia Fuller (2014), tratando do tema sobre direito penal difuso, notadamente na sociedade da informação:

> Assim, para além dos inegáveis efeitos positivos trazidos à sociedade, o advento das novas tecnologias, em especial da internet, dada a vulnerabilidade dos limites de seu uso, pode impor violações ao bem estar individual e coletivo, bem como a valores constitucionais, visto ser considerado, muitas vezes, pelo autor do crime como um mundo situado extramuros do real (e, portanto, metajurídico). E, em meio a este pensamento, a internet passa a ser compreendida de forma ilegítima como artefato para o cometimento de crimes contra direitos humanos, como v.g. neonazismo digital, ciberterrorismo, ciberbullying etc.

Vê-se que se trata de uma criminalidade específica, quer em razão do *modus operandi*, sujeitos ativos e passivos, resultados com a nota da transnacionalidade em muitos casos. Certo é que os bens jurídicos violados são de estatura constitucional como a liberdade, intimidade, privacidade, honra, imagem, tendo como base nuclear o direito à segurança informacional que acaba sendo violada em um de seus elementos caracterizadores.

2. Meio ambiente digital, sua significação e contextualização constitucional

Segundo aspectos do meio ambiente, de acordo com uma divisão didática, observa-se a existência do meio ambiente natural, laboral, artificial e cultural, cada qual, com o seu acento constitucional.

A ambiência digital deve ser considerada tendo base constitucional, visto que a sua gênese se encontra no art. 216 da CF. Nessa esteira, Celso Antonio Pachecho Fiorillo (2015, p.143) afirma que:

> o meio ambiente cultural manifesta-se em nosso país em face de um cultura que passa por diversos veículos reveladores de novo processo civilizatório adaptado necessariamente à sociedade da informação, a saber, de nova forma de viver relacionada a uma cultura de convergência em que as emissoras de rádio, televisão, o cinema os videogames, a internet, as comunicações por meio de ligações de telefones fixos e celulares *etc* moldam uma 'nova vida' reveladora da nova faceta do meio ambiente cultural: a saber: o meio ambiente digital.

Assim, de acordo com a interpretação sistemático-teleológica, chega-se à conclusão que as novas tecnológicas, inclusive envolvendo aspectos da inteligência artificial podem ser consideradas como patrimônio cultural, evidenciando novas formas de expressão, criações, modos de fazer e viver presentes na sociedade da informação como identificadoras de diferentes grupos formadores da sociedade brasileira que podemos denominar de coletivos digitais.

3. O microssistema jurídico-penal e os bens jurídicos tutelados no meio ambiente digital

Após a análise da subsunção do meio ambiente digital como inserido no meio ambiente cultural (sob uma visão metodológica e não holística de meio ambiente), deve-se ressaltar que pelas suas especificidades, há a necessidade de criar-se um microssistema jurídico para a sua tutela jurídica, ou seja, pensar-se em uma única estrutura normativa global, abrangendo aspectos de direito material e direito processual que conversem entre si, dialogando-se (BENJAMIM; MARQUES,, 2018) inclusive com fontes normativas de outras áreas dogmáticas.

A *ratio* inspiradora para a criação de um microssistema próprio de proteção do ambiente digital visa propiciar uma regulamentação própria, garantindo-se maior segurança jurídica e como tal, concebendo-se um tratamento sistemático a institutos distintos e dispersos em ordenamentos jurídicos e documentos interdisciplinares (e até multidisciplinares).

Um microssistema jurídico deve aproveitar as seguintes características, a saber: interdisciplinaridade; principiologia própria; sujeitos determinados, bem como, conteúdo específico e tecnolinguagem, caracterizando um modelo de coesão e unidade, partindo-se da Constituição Federal como sistema de interação com a ambiência digital.

Em relação aos critérios benéficos da construção de um microssistema, Daniel de Bittencourt Morais (2019, p.144) quando comparado à sistemática da codificação, destacando dentre outros: (i) o tratamento sistemático a institutos antes dispersos no ordenamento jurídico; (ii) a maior segurança jurídica, uma vez que trazem regras específicas ou setoriais; (iii) a regulação minudente da matéria, trazendo normas de diversos ramos do direito no mesmo diploma normativo; (iv) a possibilidade de alteração legislativa mais célere; e (v) a personalização das normas jurídicas, valorizando particularidades.

Referidas as ideias sobre o conceito e as características de microssistema digital, deve-se observar que é possível assimilar a ideia acima para a tutela penal, verificando-se que para a sua construção alguns pontos deverão ser considerados, desde um conceito ontológico sobre crime e bem jurídico informáticos; teoria geral do delito prevista no Direito Penal clássico; normatividade principiológica constitucional e infraconstitucional.

O conceito de crime informático que se utiliza como referencial pode ser inicialmente encontrado nas conclusões do Décimo Congresso das Nações Unidas sobre *Prevención del Delito y Tratamiento del Delincuente* (Viena, 10 a 17 de abril de 2000) que declara:

> Por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informacional.

Portanto, o cerne do microssistema jurídico no âmbito da tutela penal digital será pautado na consideração do denominado bem jurídico penal difuso. Assim, diante da ambiência digital, deve ser analisada a proteção de bens jurídicos coletivos lato sensu, especialmente a proteção de dados pessoais, a segurança e a autonomia informacional, segundo o previsto na Lei nº 13.709, de 14 de agosto de 2018 conhecida como Lei Geral de Proteção de Dados (LGPD)

Fácil é notar que os bens jurídicos acima citados, em sua caracterização, não apresentam aspectos de cunho individualista, posto que a violação de cada um atinge substratos sociais, econômicos e culturais, detendo a nota de essencialidade e transindividualidade.

Vale dizer que os crimes informáticos se caracterizam como delitos pluriofensivos, pois violam necessariamente os direitos referentes à intimidade, privacidade, autonomia, liberdade e informação qualificada. Entretanto, grande é a problemática envolvendo o tratamento jurídico sobre o tema crimes no meio ambiente digital, pois há notória ausência de uma regulamentação pátria específica, bem como, existência de lacunas processuais que serão analisadas em relação a dificuldades de definição de jurisdição e competência, responsabilidade penal e de colaboração processual, evidenciando e propagando a chamada "cifra negra de criminalidade"

São bens jurídicos que envolvem o caráter de carência e dignidade criminal[20] para construção de tipos penais e espaço de tratamento jurídico-penal diferenciado

[20] Os conceitos de dignidade e carência criminais foram trazidos por Von Lizt e representam respectivamente, a relevância do bem jurídico (direitos à liberdade, intimidade, isonomia, lazer, comunicação social) a ser tutelado pela esfera penal e a necessidade desta mesma tutela à sociedade. Em relação aos crimes praticados em face da sociedade da informação, é facilmente perceptível a existência de ambos os elementos acima trazidos. FULLER, Greice Patrícia. O Direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. **Anais do VII Congresso Brasileiro de**

que tutele os direitos fundamentais. É cediço que a função precípua do Direito Penal consiste na proteção jurídica da coletividade de bens jurídicos que resguardam direitos humanos, como no caso, intimidade, privacidade, proteção de dados e segurança da informação.

Portanto, observa-se que os crimes informáticos *lato sensu* (VELASCO NUÑEZ, 2006, p. 98) violam bens jurídicos relevantes e constitucionais, sendo que segundo Luigi Ferrajoli (2011, p. 12), podem ser de quatro aspectos: a. os direitos humanos, que são os direitos primários das pessoas, que dizem respeito indistintamente a todos os seres humanos, como, *v.g.* o direito à vida, à integridade da pessoa, a liberdade pessoal, a liberdade de consciência e de manifestação de pensamento, o direito à saúde e à instrução; b. os direitos públicos referentes à cidadania, como o de moradia, reunião e associação, trabalho e previdência; c. os direitos civis, elencando às liberdades negociais e de agir em juízo; d. os direitos políticos como o direito de votar e de ser votado.

Depreende-se do que acima foi mencionado que a teoria dos direitos e bens fundamentais corresponde aos bens jurídicos atingidos por grande parte de condutas produzidas no cenário informático.

Assim, vê-se a "obrigação constitucional de incriminar" , ou seja, o mandado de criminalização em termos de dignidade criminal (DOLCINI; MARINUCCI, 1994, p. 156) em face do chamado meio ambiente digital, tendo em vista que nele se impõe a necessária obediência a bens jurídicos inegavelmente de valores constitucionais, como a intimidade e autodeterminação informativa e proteção de dados (BAÓN RAMÍREZ, 1996, p. 96)

> (...) como derecho que asiste a una persona para decidir, por sí misma, de qué datos pueden disponer otros y

> en qué circunstancias, y con qué límites pueden se revelados en cuanto forman parte de su intimidad.

Exposta a necessidade de construção de um microssistema jurídico-penal, deve ser apontada a base principiológica a ser assentada. Para além dos princípios estabelecidos como ganho garantistico à pessoa humana, no Direito Penal e Processual Penal, há a observância de outros, como fulcro na Constituição Federal e na LGPD, a saber:

a) Princípio da Dignidade da Pessoa Humana:

Importante notar que a dignidade consiste em um atributo a que todos os seres humanos são titulares, não estando, portanto, condicionada a nenhum fator de *discrímen* como *v.g* conduta de uma pessoa humana ou sua peculiar situação econômica ou cultural. A reflexão sobre o citado princípio tomou assento desde Kant ao asseverar que nenhum homem pode ser tratado por outro como um simples instrumento, mas sim, como um fim em si. Trata-se de propor o expurgo da concepção de "coisificação" do humano em face de seu valor intrínseco como ser pensante e dotado de consciência e vontade.

Sobre o assunto, Ingo Sarlet (2001, p.60) estabelece:

> A dignidade é a qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, nesse sentido, um complexo de direitos e deveres fundamentais que garantem a pessoa contra todo e qualquer ato de cunho degradante e desumano (...)

Nesse mesmo sentido e em ordem complementar, Robert Spaemann (1989, p.135) afirma:

> La exigencia del respeto absoluto que la persona humana merece descansa en un fundamento que ha de ser también absoluto, y no relativo a la situación cultural o

> histórica: 'solo el valor del hombre en sí – no únicamente para los hombres – hace de su vida algo sagrado y confiere al concepto de dignidad esa dimensión ontológica sin la cual no puede pensarse siquiera lo que con ese concepto se quiere expresar.

Portanto, caso haja violação ao princípio aludido por meio de comunidade virtuais ou desrespeito à proteção de dados estabelecida desde o art. 6º da LGPD.

b) Princípio da Autonomia:

Trata-se de um princípio que impõe o dever de proibição de certas técnicas em face de apresentarem risco desproporcionais para saúde biopsicossocial, impedindo, portanto, que alguém possa ser obrigado a ser submetido a práticas de determinadas intervenções técnicas, como *v.g*. dispositivos médicos ou ter sua intimidade, privacidade e imagem violados. O princípio atualmente atrelado com os denominados neurodireitos, como identidade pessoal, livre-arbítrio, privacidade mental, acesso equitativo e proteção contra os vieses (CRESPO, 2013).

c) Princípio da Isonomia:

O princípio da isonomia subsumido à realidade da sociedade da informação traz a ideia de que todos devem ter acesso ao uso da internet, evitando-se a exclusão digital e tornando-se efetivo o citado direito humano consagrado pela Organização das Nações Unidas, destacando-se a General Conference 38 C/53, realizada pela Unesco, em 2015, na qual , em termos gerais, houve a determinação da universalização da internet. Ainda saliente-se o relatório das relatorias especiais para a Liberdade de Expressão da Assembleia Geral da ONU, de 2011, em nível global, e da Comissão Interamericana de Direitos Humanos da OEA, de 2013, em nível regional, defendendo-se a internet aberta a todos como corolário aos direitos da liberdade de expressão e livre acesso à informação dos usuários da rede.

d) Princípio da solidariedade

Os meios de tecnologia da informação, notadamente a internet, devem prestar-se a serem instrumentos de colaboração a todos, colocando à disposição da comunidade conhecimentos que não poderiam chegar de outro modo, fazendo-se mais acessível o acesso à educação, cultura, trabalho e outros direitos sociais que permitem o desenvolvimento pessoal do ser humano.

Nesse ponto é que se abre a discussão para a chamada brecha digital, pois não será possível alcançar a visão ao acesso igualitário se não forem eliminadas as desigualdades no acesso à rede

O princípio da solidariedade está em consonância com as finalidades da sociedade da informação que tem como mote principal a busca pelo bem comum, na qual se promove a igualdade, a segurança e a liberdade. Sobre o assunto, Fabio Konder Comparato (2006, p. 577) afirma que a solidariedade:

> é o fecho de abóboda do sistema de princípios éticos, pois complementa e aperfeiçoa a liberdade, a igualdade e a segurança. Enquanto a liberdade e a igualdade põem as pessoas umas diante das outras, a solidariedade as reúne, todas, no seio de uma mesma comunidade. Na perspectiva da igualdade e da liberdade, cada um reivindica o que lhe é próprio. No plano da solidariedade, todos são convocados a defender o que lhes é comum. Quanto à segurança, ela só pode realizar-se em sua plenitude quando cada qual zela pelo bem de todos e a sociedade pelo bem de cada um dos seus membros.

e) Princípio da Legalidade

Em nossos dias, uma das ameaças potencialmente mais intensas e determinantes contra à intimidade, à honra, à imagem, à incolumidade psíquica e em geral, aos direitos das pessoas, provém da manipulação e uso inadequado de dados incorporados aos meios informáticos. Por isso, houve a criação de um microssistema legal através da Lei 12965/2014, conhecida como Marco Civil da

Internet que estabelece princípios, garantias, direitos e deveres para o uso da Internet, assim como a Lei Geral de Proteção de Dados (LGPD).

Assim, em face do princípio da legalidade, o ambiente digital deve estar limitado por normas situadas no *ontos* constitucional, assim como no ordenamento jurídico infraconstitucional acima indicado sedimentadores de condutas e usos adequados dos meios de tecnologia.

f) Princípio da Liberdade

A liberdade preconizada como princípio assim o é, por ser considerada como valor superior ao ordenamento jurídico, posto que sem ela, os demais direitos não poderão ser realizados. Aqui sustentamos a ideia de liberdade como um valor central e vislumbrado sobre o aspecto da liberdade de conduzir-se e autodeterminar-se, respeitando as restrições que estejam legitimamente estabelecidas na lei constitucional e em demais ordenamentos infraconstitucionais.

Trata-se de ser a base para o exercício da segurança individual e também informática.

O direito à liberdade (e aqui se inserem os direitos à liberdade de informar, expressar e comunicar) ganhou novos contornos, a partir do momento no qual houve ampliação de suas formas de manifestações através do surgimento da sociedade da informação. O poder de comunicação implementou-se, tornando-se cada vez mais rápido e efetivo, reduzindo incontestavelmente as fronteiras territoriais que afastam o direito em comento. Contudo, essa liberdade de comunicação gerou uma inequívoca diminuição da qualidade da informação disponível, bem como, operou a redução do sentido comunicacional no que tange a interação intersubjetiva pessoal (FULLER, 2014, p. 137).

Como afirma Camacho Losa (1987, p. 13) "en todas las facetas de la actividad humana existen el engaño, la manipulación, la codicia, el ansia de venganza, el

fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano (...)"

Há duas ideias importantes sobre esse cenário para que a sociedade da informação não se converta em um espaço sufocante e controlado por quem detenha maior força material ou intelectiva. A primeira revela que se deve evitar que a sociedade da informação possa converter-se em uma sociedade anômica e não solidária, na qual cada membro busque seus próprios interesses sob o prisma do individualismo. A segunda diz respeito a sua regulamentação e ao aspecto relativo ao problema das soberanias irrenunciáveis e supervaloradas pelos Estados.

A sociedade da informação não pode servir como instrumento capaz de aniquilar a liberdade e os demais direitos individuais dos cidadãos, conhecendo que existem valores comuns na sociedade que não podem ser violados pelo uso desproporcionado e irresponsável dos meios de tecnologia de informação em um flagrante retrocesso ao estado de natureza.

Conclusões:

Ao analisar as condutas praticadas no meio ambiente digital observa-se a ofensa a bens jurídicos penais dotados da característica de serem coletivos *lato sensu*, como a proteção de dados pessoais e a segurança informacional assegurados na LGPD.

Depreende-se ainda a existência de mandados de criminalização para proteção dos bens jurídicos acima aludidos, sendo considerados implícitos, posto que a sua tutela é inegavelmente relevante e fundamental à existência digna do ser humano.

Em sendo interesses metaindividuais e sendo dotados de especial relevância ao próprio Estado Democrático de Direito, necessitam de uma proteção assegurada em um microssistema jurídico próprio que assegure o tratamento do tema de

maneira interdisciplinar, sistemática, global, pontuando-se a construção de base principiológica própria, destinatários específicos, conteúdo e institutos próprios e linguagem técnica coerente com o assunto.

Para tanto, o modelo de microssistema deverá ser dotado de coesão e unidade, dialogando com outras fontes normativas para além do Direito Penal e Processual Penal, como, *v.g.* a LGPD, extraindo seu conteúdo de validade das normas constitucionais, incluindo-se o preâmbulo que já impõe não apenas o fundamento axiológico como também limites materiais de tutela de bens jurídico-penais.

Referências

BALLESTEROS, Jesús. Repensar la Paz. Madri: Eiunsa, 2006, p. 16.

BAÓN RAMÍREZ, Rogerio. Ambito jurídico das tecnologías de la información. Cuardernos de Derecho Juridicial, XI, 1996, p. 86.

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima. A Teoria do Diálogo das Fontes e seu Impacto no Brasil: uma homenagem à Erik Jayme. Revista de Direito do Consumidor, São Paulo, v. 115, ano 27, jan./fev. 2018. Disponível em:https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1042/911. Acesso em: 16 jul. 2023.

CAMACHO LOSA, Luis. El delito informático. Madrid, 1987, p.13.

COMPARATO, Fabio Konder. Ética: direito, moral e religião do mundo moderno. São Paulo: Companhia das Letras, 2006, p. 577

CRESPO, Demetrio. Compatibilismo humanista. Una propuesta de conciliación entre Neurociencias y Derecho penal. Demetrio Crespo, E. (Dir.) / Maroto Calatayud, M. (Coord.). In:Neurociencias y Derecho penal, Madrid: Edisofe, 2013.

DOLCINI, Emílio; MARINUCCI, Giorgio. Constituição e escolha dos bens jurídicos. Revista Portuguesa de Ciência Criminal. Lisboa. Abril/junho 1994, p. 156.

FERRAJOLI, Luigi. Por uma teoria dos Direitos e dos bens fundamentais. Porto Alegre: Livraria do Advogado, 2011.

FIORILLO, Celso Antônio Pacheco. Princípios constitucionais do direito da sociedade da informação: a tutela jurídica do meio ambiente digital. São Paulo: Saraiva, 2015.

FULLER, Greice Patrícia. Os delitos e as novas tecnologias em face da relação dialógica com os direitos humanos. In: , p. 220.

FULLER, Greice Patrícia. O Direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. Anais do VII Congresso Brasileiro de Direito da Sociedade da Informação: regulação da mídia na sociedade da informação. São Paulo 16 e 17 de novembro de 2014, v. 7, ISSN 1982-6788. Disponível em file:///G:/ARTIGO%20PUB%20livro%20INGO%20Direitos%20Humanos%20e%20Fundamentais%20na%20Era%20da%20Informa%C3%A7%C3%A3o.pdf. Acesso em 19/10/2023.

HABERMAS, Jürgen. A constelação pós-nacional: ensaios políticos / Jürgen Habermas Tradução de Márcio Seligmann-Silva. São Paulo : Littera Mundi, 2001

MORAIS, Daniel de Bettencourt Rodrigues Silva. O Direito das Relações privadas dos microssistemas jurídicos: uma perspectiva luso-brasileira (?). Revista Esmat ano 11 - Nº 18, Pág. 133 - 172 | Edição Especial 2019. Disponível em: http://esmat.tjto.jus.br/publicacoes/index.php/revista_esmat/article/view/307, acesso em: 17. Jul. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Disponível em https://www.un.org/es/conf/xcongreso/prensa/2088cs.shtml. Acesso em 20/10/2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. General Conference. 38th Session, Paris, 2015. Disponível em https://unesdoc.unesco.org/ark:/48223/pf0000235614. Acesso em 14/10/2023.

PUELLES, Roberto Contreras. Inteligencia Artificial en el Sistema de Justicia. Neuroderechos y Ciberdelincuencia. Disponível em ttps://www.academia.edu/63157380/Inteligencia_Artificial_en_el_Sistema_de_Justicia_Neuroderechos_y_Ciberdelincuencia?auto=download&email_work_card=download-paper. Acesso em 13/04/2022

SARLET, Ingo Wolfgang. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988. Porto Alegre: Livraria do Advogado, 2001, p. 60.

SPAEMANN, Robert. Lo natural y lo racional. Madrid: Rialp, 1989, p. 135.

TAKAHASHI, Takeo. Sociedade da Informação no Brasil: livro verde. Org. Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000, p. 31.

VELASCO NUÑEZ, Eloy. Delitos contra y a través de las nuevas tecnologías. ¿Como reducir su impunidad? Cuadernos de Derecho Judicial, III. Madrid: Consejo General del Poder Judicial, 2006.

ZIZEK, Slavoj. Violência: seis reflexões laterais. São Paulo: Biotempo, 2014.

Microssistema do Ambiente Digital e Privacidade: Análise da Proteção Jurídica de Dados Pessoais na era da Hiperexposição na Sociedade da Informação

Irineu Francisco Barreto Junior e Samyra Haydêe Dal Farra Naspolini

Introdução

A Sociedade da Informação vem impondo, nas últimas duas décadas e meia, inúmeros desafios advindos da migração do real para o virtual de parcela significativa da sociabilidade humana, dos efeitos da transformação dos dados pessoais em mercadoria e da hiperexposição dos usuários das plataformas digitais e Tecnologias de Comunicação e Informação – TICs. A construção de um arcabouço jurídico – global e local – que ressignifique e proteja a privacidade ocupa elevada posição entre esses desafios.

Nesse cenário o Brasil vem envidando esforços na arquitetura de um conjunto de normas que amoldam um legítimo Microssistema do Ambiente Digital, que pode ser compreendido com um ecossistema de conexão entre regras jurídicas cujo cerne reside no estabelecimento de sinergia entre diplomas legais que se complementam e, ainda, em proporcionar a aplicação de dispositivos dos códigos complementares e harmonizar normas e princípios que tutelam diferentes direitos.

No caso do Microssistema do Ambiente Digital voltado à proteção da privacidade dos usuários das plataformas digitais, o presente capítulo realiza uma análise interpretativa dogmática jurídica da Lei 12.965/2014, de 23 de abril de 2014 – denominada Marco Civil da Internet – e Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, institutos jurídicos que complementam a Constituição Federal de 1988 e atualizam a carta constitucional

brasileira frente aos novos delineamentos históricos advindos com a Sociedade da Informação.

A abordagem situa-se no contexto da Sociedade da Informação, advento contemporâneo que produz forte repercussão no ecossistema jurídico, tendo em vista que as plataformas digitais dissolveram as fronteiras entre o real e o virtual provocando a hiperexposição dos usuários e inúmeros outros efeitos como a erosão da privacidade e a necessidade de estabelecer parâmetros para o tratamento de dados pessoais.

O escopo epistemológico do estudo adota a linha jurídico-dogmática que considera o direito com autossuficiência metodológica e trabalha com os elementos internos ao ordenamento jurídico. Essa abordagem desenvolve investigações com vistas à compreensão das relações normativas nos vários campos do direito e com a avaliação das estruturas interiores ao ordenamento jurídico. Concomitantemente acentua a noção de eficiência e eficácia das relações entre e nos institutos jurídicos restringindo a análise do discurso normativo aos limites do ordenamento. Isto não significa que deve estar voltado apenas para o interior do ordenamento ou ali enclausurado (Gustin; Dias; Nicácio 2020, p. 20-25).

Globalização e Sociedade da Informação

Fenômeno da Pós-Modernidade, a Globalização foi possível principalmente devido aos avanços nos meios de comunicação que tiveram início nos anos de 1970. Refere-se às transformações ocorridas ao redor do globo, em virtude da rapidez da comunicação propiciada pelas novas tecnologias.

Para Ulrick Bech[21] globalização significa "os processos, em cujo andamento os Estados nacionais veem a sua soberania, sua identidade, suas redes de

[21] BECK, Ulrich. O que é globalização? Equívocos do globalismo- respostas à globalização. Tradução André Carone. São Paulo: Paz e Terra, 1999, p. 30.

comunicação, suas chances de poder e suas orientações sofrerem a interferência cruzada de atores transnacionais".

Neste contexto de globalização, muitos autores especificam a chamada Sociedade da Informação, identificada, segundo Barreto Junior[22] como as "modificações da sociedade contemporânea trazidas pelas novas tecnologias, com especial foco à produção e uso da informação".

Conforme Roberto Senise Lisboa[23], trata-se do período histórico em que a informação prevalece sobre os meios de produção e distribuição dos bens. Nas palavras do autor:

> "Sociedade da informação", também denominada de "sociedade do conhecimento", é expressão utilizada para identificar o período histórico a partir da preponderância da informação sobre os meios de produção e a distribuição dos bens na sociedade que se estabeleceu a partir da vulgarização das programações de dados utiliza dos meios de comunicação existentes e dos dados obtidos sobre uma pessoa e/ou objeto, para a realização de atos e negócios jurídicos[24].

Importante frisar que a Sociedade da Informação faz surgir "complexas redes profissionais e tecnológicas voltadas à produção e ao uso da informação, que alcançam ainda sua distribuição através do mercado, bem como as formas de utilização desse bem para gerar conhecimento e riqueza"[25].

Para Takahashi a Sociedade da Informação é um fenômeno global que traz uma profunda mudança nas atividades sociais e econômicas, havendo quem a considere "um novo paradigma técnico-econômico"[26]. Neste contexto de sociedade da informação, globalizada, a tecnologia e a comunicação se tornaram

[22] BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). **O Direito na Sociedade da Informação**. São Paulo: Atlas, 2007.
[23] LISBOA, Roberto Senise. Direito na sociedade da informação. Revista dos Tribunais, v. 95, n. 847, 2006, p. 115
[24] *Ibid.*
[25] BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). **O Direito na Sociedade da Informação**. São Paulo: Atlas, 2007, p. 2.
[26] TAKAHASHI, Tadao. **Sociedade da informação no Brasil**: livro verde. Ministério da Ciência e Tecnologia (MCT), 2000, P.5.

aspectos centrais do desenvolvimento social, gerando novas formas de violações de direitos fundamentais nas relações públicas e privadas, exigindo um arcabouço legal de proteção específico.

Marco Civil da Internet

A lei 12.965/2014 – denominada Marco Civil da Internet – é uma resposta do poder legislativo brasileiro aos conflitos surgidos com a disseminação da Sociedade da Informação. Expressa a resposta do legislador, entre outros aspectos advindos da convergência digital e da disseminação em escala mundial da internet, para avançar na proteção da privacidade e dos dados pessoais na rede[27]. O MCI destaca nas suas Disposições Preliminares e Princípios:

> Disposições Preliminares.
> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> (...)
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> Princípios.
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> (...)

Desde o início, nas suas disposições iniciais o Marco Civil da Internet reitera o compromisso do país com os princípios dos direitos humanos em contexto internacional. Também faz menção à dicotomia entre direitos fundamentais e direitos absolutos ao garantir a liberdade de expressão, tendo em consideração a

[27] BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015. p. 100-127.

proteção da privacidade e dos dados pessoais dos usuários da rede. É de suma importância abordar essa dualidade, que é inerente à sobreposição histórica entre direitos fundamentais e reconhecer a possível ampliação dessa dicotomia devido às mudanças na sociedade da Informação, paradigma atual de desenvolvimento do capitalismo, superando as antigas dicotomias entre sociedade, economia, cultura e comunicação informática, e moldando assim um novo estágio no desenvolvimento do sistema econômico.

O Marco Civil almeja assim, nas disposições preliminares e nos seus princípios, imiscuir-se nos paradoxos colocados pela sociedade em rede frente ao princípio da dignidade da pessoa humana. Neste aspecto reside o foco do Marco Civil: as transformações que a sociedade da informação provocou na compreensão e no exercício dos denominados direitos fundamentais. Especialmente nos direitos sobre privacidade e intimidade, uma vez que a atuação dos meios de comunicação midiáticos interfere, decisivamente, nos processos de sociabilidade, frente ao exercício da liberdade de expressão[28].

Esta é uma das complexas questões contemporâneas em uma era de hiperexposição dos usuários das plataformas digitais: o progresso tecnológico introduz novas dimensões ao debate sobre a dicotomia entre os benefícios da livre circulação de informações e o direito à preservação da intimidade, incluindo o direito de não ser informado e de não saber.

É possível situar, nessa perspectiva, a dicotomia entre liberdade de circulação de informações e preservação da privacidade, na aludida assimetria entre direitos absolutos e fundamentais, nesse novo cenário de circulação incessante de informações provocado pelo avanço tecnológico. Assim, é defensável situar o Marco Civil entre as principais proteções da privacidade e da intimidade frente ao

[28] BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015. p. 100-127.

ritmo desenfreado da hiperexposição de usuários da rede impulsionada pela circulação de informações advinda do avanço tecnológico.

Não é sem fundamento, portanto, que a referida legislação tenha gerado efeitos favoráveis na solução de conflitos advindos da rede, tal como assinala Florêncio Filho: "o Marco Civil da Internet, apesar de suas imperfeiçoes, foi um importante passo simbólico para afirmar os direitos e garantias dos usuários da internet e reafirmar as obrigações dos provedores na rede mundial de computadores".[29] Para tal finalidade, no Capítulo II, dos Direitos e Garantias dos Usuários, o Marco Civil expressa, *in verbis*:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> (...)
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

[29] FLORÊNCIO FILHO, Marco Aurélio. Liberdade de Expressão e a Violação de Privacidade. In: DEL MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coords.). **Marco Civil da Internet: lei 12.965/2014**. São Paulo: Editora Revista dos Tribunais, 2014, p.40.

> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Esse conjunto de aspectos do Art. 7º, voltados à proteção e inviolabilidade da privacidade, da intimidade e da vida privada, busca oferecer respostas aos inúmeros registros de utilização indevida de dados pessoais de usuários da rede e outros conflitos que advém da utilização das plataformas digitais. O referido artigo determinou que o sistema adotado pelo nosso ordenamento jurídico para ciência do usuário fosse denominado o*pt-in*[30]. Neste modelo, o usuário deverá consentir de forma expressa e inequívoca, quanto ao tratamento dos seus dados pessoais. Por outro lado, o sistema *opt-out* (não adotado em nosso sistema) prevê que o usuário deve manifestar de forma expressa o seu interesse em sair, isto porque, o pressuposto é de concordância automática.

Entende-se correto o consentimento genuíno do usuário, sobretudo quando *expresso, livre, específico e informado*. É cediço que os prestadores de serviços no ambiente virtual, na maioria das vezes, não proveem a possibilidade de atendimento ao dispositivo. Isso porque a mera condição de clicar em um botão com a legenda *"Li e aceito os termos de uso"*, obviamente, não é suficiente a esta condição. Hoje, aplicativos disponíveis para *smartphones* informam quais dados serão coletados para que o usuário autorize sua instalação.

Prossegue o Marco Civil, ainda no Capítulo II, em seu Art. 8º., ao reafirmar o valor da proteção da privacidade e da intimidade, estabelecer a diretriz da proteção dos dados pessoais e determinar a existência de regras contratuais claras que assegurem o sigilo das comunicações privadas pela internet:

[30] BARRETO JUNIOR, Irineu Francisco; SAMPAIO, Vinícius Garcia Ribeiro; GALLINARO, Fábio. Marco civil da internet e o direito à privacidade na sociedade da informação. **Direito, Estado e Sociedade**, n.52, p. 114 a 133, jan/jun. 2018.

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

A abordagem da privacidade e da proteção dos dados pessoais na lei 12.965/2014, Capítulo III, Seção II, normatizou aspectos importantes da *Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas*. Dentre os quais, destaca-se, *in verbis (suprimidos os respectivos parágrafos)*:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> (...)
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Revela-se que a proteção dos registros, dados e comunicações privadas e seus aspectos tecnológicos, é concatenada de forma inequívoca com os princípios da lei 12.965/2014. Essa é uma das principais características do Marco Civil da Internet, tratar-se de uma legislação mais principiológica, do que meramente procedimental. Na perspectiva sociológica, responde, ainda, a outras funções que o Direito exerce em sociedade, voltadas ao exercício das funções educativas e preventivas que o fenômeno jurídico reflete nos tempos presentes.

Malgrado o Marco Civil da Internet seja formalmente uma lei infraconstitucional[31], que deve se pautar pela Constituição Federal, é importante reconhecer seu conteúdo de direitos fundamentais, caracterizado não somente pelo rol constitucional nele compreendido, mas também por seu caráter diretivo, garantidor de direitos. Acreditamos que este estudo sobre a privacidade na Sociedade da Informação, embora discreto, possa contribuir para fomentar a discussão inerente à proteção de dados na internet, tema cuja importância nos provoca a continuar e desenvolver esta pesquisa.

Lei Geral de Proteção de Dados

A vigilância on-line advinda da Sociedade da Informação é cada vez mais intensa sobre os usuários da rede mundial de computadores, percepção que tem sido disseminada, mesmo que de forma ainda difusa, entre os usuários das tecnologias informáticas. Esse movimento acarreta na hiperexposição dos usuários das plataformas digitais que dissolve as barreiras entre real e virtual, público e privado.

A resposta oferecida pelo poder legislativo brasileiro para mitigar a superexposição daqueles que se utilizam das ferramentas tecnológicas e, como contrapartida, cedem seus dados pessoais para fins de tratamentos múltiplos, reside na Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.

O *ethos* da LGPD é orientado à *autodeterminação do usuário, legítimo titular dos dados pessoais, quanto à aplicação e tratamento aos quais serão submetidos seus registros informáticos*. Essa autodeterminação repousa na necessidade de

[31] BARRETO JUNIOR, Irineu Francisco; SAMPAIO, Vinícius Garcia Ribeiro; GALLINARO, Fábio. Marco civil da internet e o direito à privacidade na sociedade da informação. **Direito, Estado e Sociedade**, n.52, p. 114 a 133, jan/jun. 2018.

manifestação expressa de consentimento e esclarecimento do titular dos dados pessoais quanto à autorização para destinação dos seus rastros digitais. Bioni[32] assinala que a análise dos princípios e a maneira pela qual a LGPD disseca o consentimento ao longo do seu corpo normativo "acabam por revelar uma forte preocupação (...) sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais". Ainda segundo Bioni, "o consentimento deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral". Na sua leitura da LGPD:

> Grande parte dos seus princípios tem todo seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio dos quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento dos seus dados e, ainda ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais modernos, como adequação e necessidade, em que o tratamento dos dados deve responder às legítimas expectativas do seu titular.[33]

O rol de fundamentos da LGPD, expressos no seu artigo 2º, apontam taxativamente para os preceitos basilares da proteção da privacidade e avançam conceitualmente até a autodeterminação do titular dos dados. Expressam *in verbis*: "I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

A LGPD avança, no rol do seu artigo 5º, em importantes definições sobre dados pessoais, dados sensíveis e anonimizados, titularidade, tratamento e consentimento – sem os quais é inviável assegurar os parâmetros mínimos de

[32] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais*:* a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019, p. 134.
[33] *Ibid*, p. 136.

proteção da privacidade e voltados a assegurar o protagonismo dos usuários quanto às suas pegadas digitais.

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> (...)
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (...).

A privacidade torna-se cada vez mais desafiadora uma vez que se perdeu, com a tecnologia, a possibilidade de assegurar a diferença entre pessoa identificada e identificável. A dicotomia entre dados anônimos (sigilosos) e dados pessoais identificáveis não é mais viável em decorrência do aparato tecnológico e das técnicas de *linkage* de bancos de dados, além do georreferenciamento que mapeia a distribuição geográfica dos dados ao monitorar a circulação dos smartphones.

Quanto ao tratamento enquanto técnica cuja implementação transforma os dados, de meros registros informáticos em informação, a LGPD o define como" toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (LGPD, 2018, artigo 5º).

O artigo sexto determina que as atividades de tratamento de dados pessoais deverão observar a boa-fé, ser pautado por princípios que assegurem seus propósitos legítimos e cujas finalidades sejam informadas ao titular, com tratamento limitado ao mínimo necessário para a realização de suas finalidades e determinações que assegurem a qualidade dos dados, transparência e segurança na sua armazenagem e tratamento. Reza ainda que devam ser adotadas medidas preventivas que mitiguem a ocorrência de danos em virtude do tratamento de dados pessoais. Ainda nesse artigo, determina que os dados não sejam tratados em aplicações que possam gerar discriminação (tratamento para fins discriminatórios ilícitos ou abusivos) e ainda a necessidade de responsabilização e prestação de contas pelo agente que promove o tratamento dos dados pessoais.

A ratificação da autodeterminação do titular como requisito para tratamento de dados pessoais ressurge no artigo sétimo da LGPD. Este somente poderá ser efetuado mediante o fornecimento de consentimento pelo titular, determina o inciso que ocupa o degrau superior da topografia do referido artigo.

Bioni afirma que franquear ao cidadão o controle sobre seus dados pessoais é eixo encontrado pela referida lei para conciliar o rol de fundamentos e determinações nela contido[34]. O autor afirma que "tão importante quanto este elemento volitivo é assegurar que o fluxo informacional atenda suas legítimas expectativas". Somadas estas ao intuito de preservação dos seus direitos de personalidade, têm-se uma interpretação do *ethos* da LGPD com a missão de mitigar a erosão da privacidade assistida na Sociedade da Informação.

[34] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais*:* a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019, p. 110.

Na LGDP o consentimento é figura central e aparece em inúmeros artigos, seguindo as previsões pretéritas do Marco Civil da Internet e a tendência mundial de conceder ao cidadão a responsabilidade de resguardar a proteção dos seus dados pessoais. No inciso I do artigo sétimo a LGPD é taxativa em afirmar que:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - Mediante o fornecimento de consentimento pelo titular; (grifos nossos)

O artigo sétimo trata, portanto, de dois conceitos centrais na LGPD, o *consentimento*, detalhado no artigo oitavo e o *tratamento* de dados pessoais, regulado no artigo nono. Conforme visto anteriormente nas definições trazidas pelo artigo quinto, para os fins da LGPD considera-se consentimento: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". (Inciso XII) e tratamento:

> X – (...) toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (Art. 5º LGPD)

Conforme estas disposições e as determinações do artigo oitavo a LGPD vai exigir que o consentimento previsto no inciso I do art. sétimo deverá ser "fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (*caput*). No caso do consentimento por escrito, a cláusula que o confere deve estar destacada das demais atribuições do contrato (§ 1º) e o § 4º veda, sob pena de nulidade, as autorizações genéricas, devendo o consentimento referir-se a finalidades determinadas. Por fim, os parágrafos 5º e 6º garantem que o consentimento pode ser revogado a qualquer tempo pelo seu titular.

No artigo nono a questão fulcral é a transparência das informações do tratamento de dados de tal maneira que "o titular tem direito ao acesso facilitado

às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva" (*caput*), referindo-se essas informações à finalidade específica do tratamento (I), à forma e duração do mesmo (II), identificação e informações de contato do controlador (III e IV), ao uso compartilhado quando houver (V), às responsabilidades dos agentes que realizarão o tratamento (VI) e os direitos do titular que devem ser mencionados de forma explícita (VII).

O § 1º do artigo nono volta a tratar da questão do consentimento, prevendo a nulidade do mesmo nos casos em que as informações oferecidas ao titular "tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca."

Também se referindo ao consentimento, o § 2º adverte que se houver mudança de finalidade para o tratamento de dados, nas situações em que esse consentimento é requerido, tal mudança deverá ser informada ao titular podendo este revogar o consentimento, se não assentir com a alteração.

Dessa forma perante a Sociedade da Informação e a erosão global da privacidade, no Brasil e no mundo, as comunidades jurídicas têm desenvolvido elementos normativos com o intuito de mitigar os efeitos derivados da economia de dados. São perceptíveis as expectativas empenhadas na Lei Geral de Proteção de Dados brasileira nesse sentido.

Considerações Finais

A Sociedade da Informação, ao inovar a lógica comunicacional no mundo requer do Direito o olhar atento aos conflitos entre garantias como privacidade, liberdade e informação. A desnecessidade da repetição de direitos e da mera subsunção expressa à internet, sob o ponto de vista lógico, sugere o caráter mais

político que jurídico da Sociedade da Informação, que aponta a necessidade de tutela jurídica dos fenômenos ocorridos na rede.

Nesse contexto, é notório no Brasil um movimento de aperfeiçoamento da voltadas à proteção de dados pessoais e manutenção de um ambiente virtual mais ético e transparente. Destaca-se nesse ecossistema o Marco Civil da Internet e a Lei Geral de Proteção de Dados (Lei 13.709, de 14 de agosto de 2018). Evidente que a efetividade deste arcabouço ainda demorará a ser plenamente aferida, mas é inegável seu teor significativamente voltado à proteção da privacidade dos usuários da rede mundial de computadores.

Nenhuma medida terá efetividade, porém, se não houver também uma mudança no padrão de utilização da internet pelos usuários. O ambiente virtual deve preservar os paradigmas do real. É inegável a necessidade do consenso sobre os princípios normativos para a proteção da privacidade, dignidade e, por reflexo, da mitigação dos efeitos da superexposição de dados pessoais que resultam da utilização da internet. Antes do estabelecimento desses consensos e da conscientização dos usuários quanto ao uso adequado da rede, o Brasil edifica um microssistema jurídico digital de relevância, significado e aplicabilidade voltado a solucionar conflitos advindos da sociabilidade humana em meio digital.

Referências

BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). O Direito na Sociedade da Informação. São Paulo: Atlas, 2007.

BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO,

Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). Direito & Internet III. São Paulo: Quartier Latin, 2015. p. 100-127.

BARRETO JUNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe Dal Farra. Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais. Cadernos Adenauer XX (2019), nº3 Proteção de dados pessoais: privacidade versus avanço tecnológico Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019.

BARRETO JUNIOR, Irineu Francisco; SAMPAIO, Vinícius Garcia Ribeiro; GALLINARO, Fábio. Marco civil da internet e o direito à privacidade na sociedade da informação. Direito, Estado e Sociedade, n.52, p. 114 a 133, jan/jun. 2018.

BARRETO JUNIOR, Irineu Francisco; VENTURI JUNIOR, Gustavo. Inteligência Artificial e seus efeitos na Sociedade da Informação. *In*: LISBOA, Roberto Senise (Org.). O Direito na Sociedade da Informação V.4. São Paulo: Almedina, 2020.

BARRETO JUNIOR, Irineu Francisco; VIGLIAR, José Marcelo Menezes. As funções da jurisprudência na Sociedade da Informação. Rev. Fac. Direito UFMG, Belo Horizonte, n. 73, pp. 391-417, jul./dez. 2018.

BECK, Ulrich. O que é globalização? Equívocos do globalismo- respostas à globalização. Tradução André Carone. São Paulo: Paz e Terra, 1999.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais*:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura. Volume I, a sociedade em rede. 5. ed., São Paulo: Paz e Terra, 2001.

FLORÊNCIO FILHO, Marco Aurélio. Liberdade de Expressão e a Violação de Privacidade. In: DEL MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coords.). Marco Civil da Internet: lei 12.965/2014. São Paulo: Editora Revista dos Tribunais, 2014, p.40.

GUSTIN, Miracy Barbosa de Souza; DIAS, Maria Teresa Fonseca; NICÁCIO, Camila Silva. (Re)pensando a pesquisa jurídica. 5. ed. ver., ampl. e atual. São Paulo: Almedina, 2020.

LISBOA, Roberto Senise. Direito na sociedade da informação. Revista dos Tribunais, v. 95, n. 847, 2006.

SARLET, Ingo Wolfgang. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988. 3.ed. Porto Alegre: Livraria do Advogado, 2004.

TAKAHASHI, Tadao. Sociedade da informação no Brasil: livro verde. Ministério da Ciência e Tecnologia (MCT), 2000.

RESPONSABILIDADE CIVIL NO MICROSSISTEMA

Jorge Shiguemitsu Fujita

1. Conceito de responsabilidade civil

O conceito de responsabilidade civil no direito romano, como bem aponta Alvino Lima, tinha "seu ponto de partida na vingança privada, forma primitiva, selvagem, talvez, mas humana, da reação espontânea e natural contra o mal sofrido; solução comum a todos os povos nas suas origens, para a reparação do mal pelo mal"[35]. Isso decorria da pena de Talião, contida na *Lex Duodecim Tabularum* (Lei das XII Tábuas), especificamente na Tábua VIII, 2ª lei. A este período vem a suceder o da composição tarifada, que fixava, em casos concretos, o valor da pena a ser paga pelo ofensor, traduzindo-se, pois, uma composição obrigatória[36]. Ainda não se cogitava da culpa[37].

Embora muitos afirmem que a responsabilidade civil teve o seu nascedouro na *Lex Aquilia de damno*, onde se tem a ideia de culpa, Giselda Maria Fernandes Novaes Hironaka[38] esclarece que não há razão para confundir o instituto contemporâneo da responsabilidade civil, fundada em um dever de compensação baseado na culpa do agente diante de ter ofendido direito alheio, com a obrigação preconizada pela *Lex Aquilia de damno*, consistente em reparar a outrem um bem ou direito, em virtude da culpa, por ter ofendido este bem ou este direito. Isso porque, embora a ideia de culpa esteja concebida em ambos os casos, como fundamento de determinação do dever, no caso da *Lex Aquilia*, a culpa é índice de

[35] LIMA, Alvino. Culpa e Risco. São Paulo: Revista dos Tribunais, 1960, p. 20.
[36] Idem, ibidem, p. 20.
[37] GONÇALVES, Carlos Roberto. Responsabilidade Civil. 15. ed. São Paulo: Saraiva, 2014, p. 47.
[38] HIRONAKA, Giselda Maria Fernandes Novaes. Responsabilidade Pressuposta. Belo Horizonte: Del Rey, 2005, p. 28-30.

obrigação, mas não é, sozinha, causa de dever, pois este depende de ser exigido por quem se sente lesado. De outra parte, no direito atual, que se ampara na teoria da culpa, existe uma simultaneidade entre culpa e dever[39]. Assim, Giselda Hironaka conclui tratar-se a responsabilidade civil de um instituto contemporâneo, surgido apenas ao término do século XVIII, com a Revolução Francesa, tendo a sua primeira formulação expressa no sistema jurídico do Código Civil da França de 1804, o qual simbolizou um modelo para as codificações de outros países.

Nos dias de hoje, para Sergio Cavalieri Filho, a responsabilidade civil é "um dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário"[40], que, a seu ver, é a obrigação.

De outra parte, Carlos Roberto Gonçalves afirma que a "responsabilidade civil é a consequência jurídica patrimonial do descumprimento da relação obrigacional"[41]. Esclarece ainda que a obrigação "é sempre um dever jurídico originário", ao passo que a "responsabilidade civil é um dever jurídico sucessivo, consequente à violação do primeiro"[42].

Para Álvaro Villaça Azevedo, responsabilidade civil é "a situação de indenizar o dano moral ou patrimonial, decorrente de inadimplemento culposo, de obrigação legal ou contratual, ou imposta por lei, ou, ainda, decorrente do risco para os direitos de outrem"[43].

O instituto da responsabilidade civil, assinala Álvaro Villaça Azevedo, encontrava-se, até há bem pouco tempo atrás, relegada a um segundo plano dentro do campo de estudos jurídicos, tendo sido somente no século XX alçado a uma condição de importância, em virtude do número cada vez maior de acidentes e do crescimento das atividades perigosas desenvolvidas pelo ser humano, sempre

[39] Idem, ibidem, p. 30 e 31.
[40] CAVALIERI FILHO, Sergio. Programa de Responsabilidade Civil. 7. ed. São Paulo: Atlas, 2007, p. 2.
[41] GONÇALVES, Carlos Roberto. Direito Civil Brasileiro. 12. ed. São Paulo: Saraiva, 2017, p. 21, v. 4.
[42] Idem, ibidem, p. 21.
[43] AZEVEDO, Álvaro Villaça. Teoria Geral das Obrigações e Responsabilidade Civil. 12. ed. São Paulo: Atlas, 2011, p. 244.

no afã de obter, de maneira desenfreada, o progresso tecnológico e econômico. Essa constatação e essa preocupação foram demonstradas na década de 1930 na França, por Louis Josserand[44].

2. Regimes jurídicos da responsabilidade civil

Temos dois regimes jurídicos da responsabilidade civil: a subjetiva e a objetiva.

A responsabilidade civil subjetiva é aquela fundada na culpa. Esta, para Alvino Lima, "é um erro de conduta, moralmente imputável ao agente e que não seria cometido por uma pessoa avisada, em iguais circunstâncias de fato"[45]. Para Anderson Schreiber, "a culpa é, inegavelmente, a categoria nuclear da responsabilidade civil concebida pelos juristas da Modernidade"[46].

São requisitos essenciais para o regime jurídico da responsabilidade civil subjetiva: a) o ato ou omissão violadora do direito de outrem; b) o dano produzido por esse ato ou omissão; c) a relação de causalidade entre o ato ou omissão e o dano; d) a culpa.

Todavia, verificou-se, pelo passar do tempo, que a responsabilidade, calcada somente na culpa do agente e, portanto, considerada subjetiva, não era suficiente para atender ao aumento da complexidade da vida, não apenas com as novas conquistas da ciência e a diversificação das atividades profissionais, mas também com um novo universo de situações que clamavam a necessidade de se proteger a vítima, aliada às dificuldades diuturnas de se promover a prova da causa dos

[44] JOSSERAND, Louis. Evolução da responsabilidade civil. Conferência pronunciada em Faculdades de Direito e Institutos de Lisboa, Coimbra, Belgrado, Bucarest, Oradéia, Bruxelas, Madri, Rabat e Casablanca, publicada em Revolutions et Actualités. Traduzida por Raul Lima. Paris: Sirey, 1936.
[45] LIMA, Alvino. Op. cit., p. 22.
[46] SCHREIBER, Anderson. Novos Paradigmas da Responsabilidade Civil. 2. ed. São Paulo: Atlas, 2009, p. 12.

acidentes causadores de danos e dela se deduzir a culpa[47]. Nesse sentido, Caio Mário da Silva Pereira advertia que a vítima não conseguia, muitas vezes, vencer a barreira processual, não logrando convencer a Justiça da imputabilidade do agente e, deste modo, não obtendo o ressarcimento desejado. Daí então o surgimento da responsabilidade civil objetiva, baseada no risco, em que se traduzia desnecessária a prova da culpa. Para Sergio Cavalieri Filho, a "doutrina do risco pode ser, então, assim resumida: todo prejuízo deve ser atribuído ao seu autor e reparado por quem o causou, independentemente de ter ou não agido com culpa"[48].

José Cretella Junior promove a distinção entre a culpa e o risco:

> [...] a culpa é vinculada ao homem, o risco é ligado ao serviço, à empresa, à coisa, ao aparelhamento. A culpa é pessoal, subjetiva; pressupõe o complexo de operações do espírito humano, de ações e reações, de iniciativas e inibições, de providências e inércias. O risco ultrapassa o círculo das possibilidades humanas para filiar-se ao engenho, à máquina, à coisa, pelo caráter impessoal e o objetivo que o caracteriza"[49].

Na responsabilidade civil objetiva, Álvaro Villaça Azevedo[50] vislumbra duas categorias: a pura e a impura. A pura é a responsabilidade civil que resulta em ressarcimento, mesmo que não haja culpa de qualquer dos envolvidos no evento. Ocorrendo a responsabilidade civil objetiva pura não há que se falar em direito de regresso em favor daquele que pagou a indenização. Já a responsabilidade civil

[47] LIMA, Alvino. Op. cit., p. 113 e 114.
[48] CAVALIERI FILHO, Sergio. Op. cit., p. 128.
[49] CRETELLA JUNIOR, José. Comentários à Constituição brasileira de 1988, Rio de Janeiro: Forense Universitária, 1991, p. 1.019, v. 2.
[50] AZEVEDO, Álvaro Villaça. Op. cit., p. 250.

objetiva impura é aquela que possui, como substrato, a culpa de um terceiro, atrelado à atividade da pessoa que promoveu o pagamento da indenização. Portanto, nessa modalidade, cabe direito de regresso.

3. Modalidades de risco

A respeito do risco existem algumas teorias: a do risco integral, do risco-proveito, do risco profissional, do risco excepcional e do risco criado.

A teoria do risco integral sustenta a posição de que "o Estado deve responder pela conduta comissiva do agente em qualquer hipótese, não se admitindo qualquer excludente de nexo de causalidade, uma vez que se exige apenas a prova do prejuízo do cidadão"[51]. O dever de indenizar se configura apenas com a existência do dano, ainda nos casos de culpa exclusiva da vítima, fato de terceiro, caso fortuito ou força maior[52].

A teoria do risco-proveito é aquele que responsabiliza aquele que tira proveito da atividade danosa, "com base no princípio de que, onde está o ganho, aí reside o encargo"[53]. O núcleo da ideia é de que o dano dever objeto de reparação por aquele que obtém algum proveito ou vantagem do fato lesivo. A teoria do risco-proveito foi adotada pelo Código de Defesa do Consumidor, justificando, deste modo, a responsabilidade civil objetiva dos fornecedores de produtos e de serviços[54].

Pela teoria do risco profissional, haverá o dever de indenizar sempre que o dano for resultante de acidentes dos quais forem vítimas os empregados no trabalho ou por ocasião dele, mesmo que não haja culpa do empregador[55]. Pode-

[51] TARTUCE, Flávio. Responsabilidade Civil Objetiva e Risco: a teoria do risco concorrente. Rio de Janeiro: Forense; São Paulo: Método, 2011, p. 128.
[52] CAVALIERI FILHO, Sergio. Op. cit., p. 130-131.
[53] Idem, ibidem, p. 129.
[54] TARTUCE, Flávio. Op. cit., p. 140.
[55] CAVALIERI FILHO, Sergio. Op. cit., p. 129.

se também falar em risco profissional quando há danos a terceiros provocados pelo próprio empregado ou preposto, em virtude do trabalho exercido[56].

Já a teoria do risco excepcional é aquela que impõe a reparação do dano, quando este decorrer de um risco excepcional, "que escapa à atividade comum da vítima, ainda que estranho ao trabalho que normalmente exerça"[57], atividade consistente, por exemplo, em trabalho em usina nuclear, na rede elétrica de alta tensão ou na manipulação de materiais radioativos.

Por último, há a teoria do risco criado, consistente na ideia de que aquele que, em virtude de "sua atividade ou profissão, cria um perigo, está sujeito à reparação do dano que causar, salvo prova de haver adotado todas as medidas idôneas a evitá-lo"[58]. Para Caio Mário da Silva Pereira, se alguém exerce determinada atividade responde pelos danos dela decorrentes em desfavor das pessoas vitimadas, independentemente do resultado bom ou mau que dela resulte para o agente[59]. Nesse sentido, a teoria do risco criado independe da vantagem ou benefício obtido pelo causador do dano, o que a distingue da teoria do risco proveito.

4. Responsabilidade civil nos microssistemas

4.1. O Código de Defesa do Consumidor – CDC (Lei nº 8.078, de 11.09.1990), que é um microssistema, adotou, com exceção da responsabilidade civil subjetiva dos profissionais liberais (CDC, art. 14, § 4º), o regime jurídico da responsabilidade civil objetiva, na modalidade risco-proveito, entendendo que o fornecedor de produto ou de serviço que expõe "a risco outras pessoas, determinadas ou não, por

[56] TARTUCE, Flávio. Op. cit., p. 162.
[57] CAVALIERI FILHO, Sergio. Op. cit., p. 129-130.
[58] PEREIRA, Caio Mário da Silva. Responsabilidade Civil. 3. ed. Rio de Janeiro: Forense, 1992, p. 24.
[59] Idem. Op. cit., p. 268.

delas tirar um benefício, direto ou não, deve arcar com as consequências da situação de agravamento"[60].

4.2. Já o microssistema da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709, de 14.08.2018) também possui o regime jurídico da responsabilidade civil objetiva na modalidade risco criado, podendo ser identificadas duas situações: a) violação de normas jurídicas do microssistema de proteção de dados; b) violação de normas técnicas voltadas à segurança e proteção de dados pessoais. Caracterizará a responsabilidade civil, se a violação da violação de norma jurídica ou técnica promover dano material ou moral a um titular ou a uma coletividade[61], independentemente da prova da culpa.

4.3. Nos dias atuais discute-se com extrema intensidade uma necessária regulação legal da Inteligência Artificial (IA), incluindo a responsabilidade civil decorrente de eventuais danos por ela ocasionados.

Em primeiro lugar, pode-se entender por Inteligência Artificial um campo da ciência da computação dedicada ao estudo e ao desenvolvimento de máquinas e programas computacionais capazes de reproduzir o comportamento humano na tomada de decisões e na realização de tarefas, desde as mais simples até as mais complexas, chegando até mesmo a aprender por meio de exemplos, tal como ocorre com a *machine learning*, ou seja, o aprendizado da máquina, com o processo de reconhecimento e reprodução de padrões feitos pela Inteligência Artificial com base na sua experiência prévia, adquirida pela utilização de algoritmos. Dentro da *machine learning* temos a *deep learning*, que se utiliza de redes neurais, as quais são unidades conectadas em rede para a análise de bancos de dados e informações, para emular o cérebro humano.

[60] TARTUCE, Flávio. Op. cit., p. 140.
[61] CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

Segundo a funcionalidade, alguns autores, como Leandro Kovacs[62], classificam as Inteligências Artificiais em a) reativas: são aquelas que funcionam com base em uma reação ao cenário dado, e não em tarefas pré-programadas ou pela memória. Esta forma é mais antiga de IA, com alta limitação; b) com memória limitada: são aquelas que funcionam, pela análise de comportamentos anteriores que ficaram gravados na memória da IA. Com base nisso, consegue tomar decisões e realizar tarefas. Máquinas com memória limitada são aquelas que, além de possuírem os recursos de máquinas puramente reativas, também são capazes de aprender com dados históricos para tomar decisões. Segundo Kovacs, "todos os sistemas atuais, como aqueles que usam o *deep learning*, são treinados por grandes volumes de dados de treinamento que são armazenados em sua memória para formar um modelo de referência para resolver problemas futuros. De *chatbots* e assistentes virtuais a veículos autônomos, todos são acionados por IA de memória limitada"[63]; c) com mente: estas se encontram em fase de desenvolvimento, tendo como função identificar e compreender as diferentes emoções, os pensamentos e os sentimentos que ocorrem no cérebro humano, melhorando as interações estabelecidas pela IA; d) autoconsciente: este tipo de IA poderia desenvolver pensamentos e emoções próprias, sem o auxílio de comandos ou algum tipo de pré-programação.[64]

Relativamente a um microssistema que regule a inteligência artificial, existem autores como Marcelo Junqueira Calixto e Stefannie Billwiller[65] que oferecem algumas hipóteses a respeito de sua responsabilidade civil, a saber:

---

[62] KOVACS, Leandro. Quais são os tipos de inteligência artificial? Disponível em: https://tecnoblog.net/responde/quais-sao-os-tipos-de-inteligencia-artificial/ Acesso em: 20.10.2023.

[63] KOVACS, Leandro. Quais são os tipos de inteligência artificial? Disponível em: https://tecnoblog.net/responde/quais-sao-os-tipos-de-inteligencia-artificial/ Acesso em: 20.10.2023.

[64] GUITARRARA, Paloma. Inteligência artificial; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/inteligencia-artificial.htm. Acesso em 20 de outubro de 2023.

[65] CALIXTO, Marcelo Junqueira Calixto; BILLWILLER, Stefannie. A Responsabilidade Civil pelos danos causados por Sistemas de Inteligência Artificial | Coluna Direito Civil. Disponível em: https://editoraforum.com.br/noticias/responsabilidade-civil-pelos-danos-causados-por-sistemas-de-inteligencia-artificial-coluna-direito-civil/ Acesso em: 20.10.2023

a) Teoria da irresponsabilidade: por essa teoria a vítima ficará sem reparação, em virtude da impossibilidade de se atribuir capacidade jurídica a uma inteligência artificial; ou, então, na ideia de que eventual reparação por danos traduziria um verdadeiro freio e desincentivo para o desenvolvimento tecnológico.

b) Teoria da responsabilidade subjetiva do programador: de acordo com essa teoria, o programador que elaborou os algoritmos iniciais responderia pelos danos causados, desde que a vítima conseguisse demonstrar a culpa do agente (programador).

c) Teoria da responsabilidade civil objetiva da IA: esta consiste na responsabilização dos *e-persons*, ou seja, uma nova categoria jurídica, em que o sistema de inteligência artificial passaria a ter personalidade e patrimônio de modo que eles responderiam diretamente pelos danos que viessem a causar. Essa teoria foi explicitamente rejeitada na apreciação pelo Parlamento Europeu sobre o tema ocorrida em 2020. Muitos pesquisadores entendem que a subjetividade legal na forma reconhecida a um ser humano é única e não pode ser reconhecida à IA, especialmente porque, pelo menos por enquanto, a IA não demonstra nenhuma evidência de ser consciente e senciente[66].

d) Teoria da responsabilidade objetiva na espécie risco-proveito: para essa teoria deverá ser responsabilizado civilmente aquele que obtém um proveito ou uma vantagem do fato lesivo.

e) Teoria da responsabilidade objetiva na espécie risco criado: por essa teoria "aquele que, em razão de sua atividade ou profissão, cria um perigo, está sujeito à reparação do dano que causar, salvo prova de haver adotado todas as medidas idôneas a evitá-lo"[67]. O conceito de risco "é o que se fixa no fato de que, se alguém põe em funcionamento uma qualquer atividade, responde pelos eventos danosos

[66] PORTUGAL, Heloisa Helena de Almeida. E-persons: Robôs inteligentes dotados de personalidade? Disponível em: https://magis.agej.com.br/e-persons-robos-inteligentes-dotados-de-personalidade/ Acesso em 19.10.2023.
[67] PEREIRA, Caio Mário da Silva. Op. cit., p. 24.

que esta atividade gera para os indivíduos"[68], independentemente da existência de culpa.

A teoria do risco criado é mais ampla que a teoria do risco-proveito, na medida em que, para a responsabilização do agente, pouco importa se houve proveito ou vantagem para ele, sendo apenas exponencial a atividade por ele exercida e que tenha criado um risco para a vítima.

Particularmente, entendemos que, para os danos causados pela Inteligência Artificial, deva ser aplicada a teoria da responsabilidade civil objetiva na espécie risco criado, e não na espécie risco-proveito (esta poderia exigir da vítima a prova da vantagem auferida pelo agente).

A responsabilidade civil objetiva na espécie risco criado foi proposta pela Resolução do Parlamento Europeu, de 20.10.2020[69], no item 8º, do Anexo B, da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à responsabilidade pela operação de sistemas de inteligência artificial[70].

BIBLIOGRAFIA REFERENCIADA

AZEVEDO, Álvaro Villaça. Teoria Geral das Obrigações e Responsabilidade Civil. 12. ed. São Paulo: Atlas, 2011.

[68] CAVALIERI FILHO, Sergio. Op. cit., p. 130.

[69] UNIÃO EUROPÉIA. Resolução do Parlamento Europeu. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020IP0276&from=PT#:~:text=Os%20cidad%C3%A3os%20devem%20ter%20o,na%20nova%20tecnologia%20seja%20refor%C3%A7ada. Acesso em: 20.10.2023.

[70] 8. Não obstante, deverá ser sempre claro que quem cria, mantém, controla o sistema de IA, ou nele interfere, deverá ser responsável pelos danos ou prejuízos causados pela atividade, o dispositivo ou o processo. Tal resulta de conceitos jurídicos gerais e amplamente aceites em matéria de responsabilidade, segundo os quais **a pessoa que cria ou mantém um risco para o público é responsável se esse risco causar dano ou prejuízo** e, por conseguinte, deverá minimizar a priori ou compensar a posteriori esse risco. Consequentemente, a ascensão dos sistemas de IA não implica uma revisão completa das regras em matéria de responsabilidade em toda a União. Para responder aos desafios relacionados com a IA, seria suficiente proceder a ajustamentos específicos da legislação existente e introduzir disposições novas bem avaliadas e orientadas, com vista a evitar a fragmentação regulamentar e a garantir a harmonização da legislação em matéria de responsabilidade civil em toda a União no que toca à IA. (negrito nosso)

CALIXTO, Marcelo Junqueira Calixto; BILLWILLER, Stefannie. A Responsabilidade Civil pelos danos causados por Sistemas de Inteligência Artificial | Coluna Direito Civil. Disponível em: https://editoraforum.com.br/noticias/responsabilidade-civil-pelos-danos-causados-por-sistemas-de-inteligencia-artificial-coluna-direito-civil/ Acesso em: 20.10.2023

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

CAVALIERI FILHO, Sergio. Programa de Responsabilidade Civil. 7. ed. São Paulo: Atlas, 2007.

CRETELLA JUNIOR, José. Comentários à Constituição brasileira de 1988, Rio de Janeiro: Forense Universitária, 1991, v. 2.

GONÇALVES, Carlos Roberto. Direito Civil Brasileiro. 12. ed. São Paulo: Saraiva, 2017, v. 4.

_____. Responsabilidade Civil. 15. ed. São Paulo: Saraiva, 2014.

GUITARRARA, Paloma. Inteligência artificial; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/inteligencia-artificial.htm. Acesso em 20 de outubro de 2023.

HIRONAKA, Giselda Maria Fernandes Novaes. Responsabilidade Pressuposta. Belo Horizonte: Del Rey, 2005.

JOSSERAND, Louis. Evolução da responsabilidade civil. Conferência pronunciada em Faculdades de Direito e Institutos de Lisboa, Coimbra, Belgrado, Bucarest, Oradéia, Bruxelas, Madri, Rabat e Casablanca, publicada em Revolutions et Actualités. Traduzida por Raul Lima. Paris: Sirey, 1936.

KOVACS, Leandro. Quais são os tipos de inteligência artificial? Disponível em: https://tecnoblog.net/responde/quais-sao-os-tipos-de-inteligencia-artificial/ Acesso em: 20.10.2023.

LIMA, Alvino. Culpa e Risco. São Paulo: Revista dos Tribunais, 1960.

PEREIRA, Caio Mário da Silva. Responsabilidade Civil. 3. ed. Rio de Janeiro: Forense, 1992.

PORTUGAL, Heloisa Helena de Almeida. E-persons: Robôs inteligentes dotados de personalidade? Disponível em: https://magis.agej.com.br/e-persons-robos-inteligentes-dotados-de-personalidade/ Acesso em 19.10.2023.

SCHREIBER, Anderson. Novos Paradigmas da Responsabilidade Civil. 2. ed. São Paulo: Atlas, 2009.

TARTUCE, Flávio. Responsabilidade Civil Objetiva e Risco: a teoria do risco concorrente. Rio de Janeiro: Forense; São Paulo: Método, 2011.

UNIÃO EUROPÉIA. Resolução do Parlamento Europeu. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020IP0276&from=PT#:~:text=Os%20cidad%C3%A3os%20devem%20ter%20o,na%20nova%20tecnologia%20seja%20refor%C3%A7ada. Acesso em: 20.10.2023.

Diálogo entre microssistemas jurídicos: ambiente digital e tutela coletiva.

Jose Marcelo Menezes Vigliar

Na primeira edição, apresentamos as bases do microssistema do ambiente digital.

Obviamente, dado o caráter inédito da proposta, o desenvolvimento doutrinário sobre o tema seguirá com importantes contribuições da comunidade jurídica.

Neste capítulo, trataremos do diálogo existente entre o microssistema digital e o microssistema da tutela jurisdicional coletiva, partindo de algumas considerações teóricas e passando para a análise das normas que tratam da reciprocidade (diálogo) entre os microssistemas.

Inicialmente, cabe lembrar que atribui-se a Natalino Irti a formulação da teoria dos microssistemas jurídicos. Na obra *L'età della decodificazione* o autor observou que na Itália, a partir dos anos 1960, teria ocorrido a promulgação de diversas leis especiais, estruturalmente favoráveis a modificações e de pretensão de duração mais efêmera, mas sem perder a essência da diciplina por ela legislada, o que era uma atitude desconhecida do sistema codificado, vocacionado a uma perenidade maior e derrogação mais difícil. [71]

Cabe uma transcrição de seu magistério[72]:

> Le leggi speciali, appropriandosi di date matetre e classi di rapporti, svuotano di contenuto la discipli- na codificata, ed

[71]Cf. IRTI, Natalino. *L'età della decodificazione*. 4ª ed. Milano: Giuffrè, 1999, p. 11.
[72]Cf. ob. cit, p. 26.

> esprimono principi che assumono una portata decisamente generale. Giunte ad un alto grado di consolidazione, le leggi speciali, apparse un tempo come mero svolgimento di disci- _pliae ge- nerali. rivelano logtchc autonome e principi organici, che dapprima si contrappongono a quelli fissati nel cod.ice civile e poi finiscono per soppiantarli del tutto. Ad una fase di conflitto segue cosi una fase defini- tiva di prevalenza e di sostituzione. Entrati in questo ciclo storico, non e pin lecito attingere i princlpi generali dal codice civile, o ragionare il problema dell'interpretazione sistematica e dell'analogia Juris nei termini classici. Occorre rompere i1 fascino del codice, e riconoscere schiettamente che le leggi spe- ciali costituiscono ormai il diritto generale di un istituto o di un'intera matéria.

Irti menciona que as leis especiais, antes tidas como um simples desenvolvimento secundário das disciplinas codificadas, passaram a revelar lógicas autônomas e orgânicas, como também reconhece Orlando Games, ao afirmar que "*ao se proliferarem, as leis especiais esvaziam o território do Código Civil [disciplina central], mutilam-no, estabelecendo uma verdadeira confrontação e usando, até mesmo, linguagem própria. [...] Passam a ser, de fato, novos centros da experiência jurídica*".[73]

Feito este breve intróito, verifiquemos o que ocorreu entre nós.

No Brasil, sobretudo nas décadas de 1960 e 1970, em que se revelou a insuficiência do Código Civil de 1916, o "Código Beviláqua", sentiu-se a necessidade de se alcançar uma maior estabilidade nas relações socioeconômicas emergentes à época e da consequente necessidade da criação de centros normativos capazes de regulá-las de forma satisfatória e segura.

[73] GOMES, Orlando. A agonia do Código Civil. *Revista de Direito Comparado Luso-brasileiro*, 1988, n. 07, pp. 01-09, p. 04.

Ainda que o fenômeno da "descodificação" esteja, inicialmente, relacionado ao direito material, também foi observado em outras disciplinas do do direito.

Para o presente, interessa-nos, sobretudo, o que ocorreu com o Direito Processual Civil.

Na ocasião, a tutela jurisdicional coletiva era, simplismente impossível, o que feria a garantia constitucional da inafastabilidade do controle jurisdicional que, na vigente Constituição Federal, está inscrita no inciso XXXV do seu art. 5º.[74]

Vejamos a contribuição de Hermes Zaneti Junior[75] que, expressamente, se refere ao direito processual, quando afirma:

> "Quando falávamos em "descodificação" e "microssistemas", geralmente debruçávamo-nos sobre o direito civil, berço desses conceitos, aos poucos fomos compreendendo a extensão também para outros ramos, como o direito administrativo, processual penal, processual civil, como o próprio microssistema do processo coletivo, que iremos analisar aqui. Mas convém advertir desde logo. O próprio direito civil começou a abordar o tema sob outra perspectiva: a da "Recodificação". No caso do direito civil tive- mos um novo Código em 2002, e muita coisa mudou. É bom frisar, contudo, que os microssistemas e a descodificação não são fenômenos exclusivos do direito civil: há, por exemplo, microssistemas penais e processuais. Além disso, o legislador, para garantir a efetividade dos diplomas normativos, muitas vezes vale-se de regras heterotópicas (de outra natureza): quando o legislador criou

[74] Cabe a transcrição da disciplina contida na Constituição Federal de 1988, dada sua grande importância:
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;

[75] Cf. Processo coletivo e Constituição: a aplicação direta do CPC/2015 ao micros- sistema dos processos coletivos. *Revista Iberoamericana de Derecho Procesal*, vol. 9, pp. 371-405, jan./jun. 2019, p. 383.

> o microssistema de defesa do consumidor, não descurou de apontar regras processuais para a efetivação dos direitos ali assegurados".

No âmbito da tutela jurisdicional, convém destacar ainda uma vez, como já iniciado na primeira edição, mas agora para relacioná-lo ao microssistema do ambiente digital, a disciplina do denominado microssistema da tutela jurisdicional coletiva, expressamente criado pelo Código de Defesa do Consumidor (Lei nº 8.078/90 de 11 de setembro de 1990) que, derrogando a denominada Lei de Ação Civil Pública (Lei nº 7.347/85 de 24 de julho de 1985) criou uma verdadeira reciprocidade entre os diploma, mediante o que se pode denominar de "normas de reenvio" existentes em ambas as leis, respectivamente em seus arts. 90 e 21.

Vejamos os textos vigentes.

Na Lei da Ação Civil Pública, encontramos o vigente art. 21, com a redação que lhe deu a lei posterior que a derrogou, ou seja, o próprio Código de Defesa do Consumidor:

> Art. 21. Aplicam-se à defesa dos direitos e interesses difusos, coletivos e individuais, no que for cabível, os dispositivos do Título III da lei que instituiu o Código de Defesa do Consumidor. (Incluído Lei nº 8.078, de 1990).[76]

Ao seu turno, vejamos a disciplina contida no art. 90 do Código de Defesa do Consumidor:

> Art. 90. Aplicam-se às ações previstas neste título as normas do Código de Processo Civil e da Lei n° 7.347, de 24 de julho

[76]. Cf.: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm#:~:text=Lei%207.347&text=LEI%20No%207.347%2C%20DE%2024%20DE%20JULHO%20DE%201985.&text=Disciplina%20a%20a%C3%A7%C3%A3o%20civil%20p%C3%BAblica,VETADO)%20e%20d%C3%A1%20outras%20provid%C3%AAncias.

> de 1985, inclusive no que respeita ao inquérito civil, naquilo que não contrariar suas disposições.[77]

Ainda na década de 1990, tive a oportunidade de desenvolver a análise, no livro Tutela Jurisdicional Coletiva (1990, p. 81-127), da disciplina legal, então vigente, e sua relação com a disciplina então inaugurada pelo Código de Defesa do Consumidor, que foi o agente da criação desse microssistema.

Em especial, gostaria de reproduzir o que referi entre as páginas 116 e 118:

> 2.4.6 Lei n° 8.078/90: O Código Brasileiro de Defesa do Consumidor: a integração dos instrumentos processuais para a realização da tutela jurisdicional coletiva
>
> Toda inovação contida no denominado Código Brasileiro de Defesa do Consumidor vem merecendo atenção da doutrina especializada, sendo certo que muito já se escreveu sobre o direito material que a Lei n° 8.078/90 disciplina de forma inovadora, havendo farta e excelente bibliografia disponível sobre todos os assuntos.
>
> O que interessa neste livro é conhecer as modificações (e foram muitas) introduzidas na disciplina da defesa dos interesses difusos, coletivos e individuais homogêneos em juízo, sendo que essa análise, de certa forma, conforme já se pôde perceber, vem sendo desenvolvida ao longo de todo este livro. Optei, como se pôde constatar, pelo método de analisar os vários institutos relacionados com a defesa dos interesses transindividuais em juízo, partindo da Lei n° 7.347/85 e, a cada inovação introduzida pelo denominado Código Brasileiro de Defesa do Consumidor, mencionar a origem.
>
> Não faria sentido comentar todas as inovações que os tópicos precedentes mencionam. Outras tantas modificações serão ainda comentadas nos tópicos subsequentes.
>
> De qualquer forma, é preciso afirmar que a Lei n° 7.347/85 e a Lei n° 8.078/90 tornaram-se diplomas recíprocos e

[77] Cf.: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

> complementares, conforme também já tive a oportunidade de acenar, e que a Lei n° 8.078/90 aprimora e eleva a tutela dos interesses transindividuais em juízo, constituindo um diploma a serviço do acesso à justiça, porque o legislador (...) ampliou sobremaneira as modalidades de interesses transindividuais passíveis de ser tutelados em juízo (...)
>
> O legislador de 1990 preocupou-se tanto com a defesa dos interesses supra individuais que entendeu por bem defini-los, com o intuito maior de não receber nenhum veto desarrazoado, que invocasse o não-amadurecimen-no das consciências jurídicas, para os novos interesses que queira, de forma expressa, defender, como o fez quando dos vetos já mencionados, que incidiriam sobre a Lei n° 7.347/85.

Na ocasião, entendi por bem apresentar, na p. 117, um quadro explicartivo com as principais alterações proporcionadas pelo Código de Defesa do Consumiror, que ora reproduzo:

> As alterações introduzidas pela Lei n° 8.078/90, repito, foram muitas, sendo certo que o quadro abaixo bem demonstra a importância do diploma ora mencionado:

Lei n° 8.078/90	Lei nº 7.347/85
art. 110	Acrescentou o inciso IV, que havia sido vetado, quando da promulgação da Lei da Ação Civil Pública
art. 111	Alterou a redação do inc. II do art. 5°
art. 112	Alterou a redação do § 3° do art. 5°
art. 113	Acrescentou §§ 4°, 5° e 6° ao art. 5°
art. 114	Alterou a redação do art. 15
art. 115	Suprimiu o caput do art. 17 da Lei n° 7.347/85, passando o parágrafo único a constituir o caput
art. 116	Alterou a redação do art. 18

A transcrição desses trechos tem o objetivo claro e inequívoco de demonstrar o acerto da doutrina de Orlando Gomes acima transcrita.

Efetivamente, "*as leis especiais esvaziam o território do Código Civil [disciplina central], mutilam-no, estabelecendo uma verdadeira confrontação e usando, até mesmo, linguagem própria. [...] Passam a ser, de fato, novos centros da experiência jurídica*".[78]

Esses novos centros da experiência jurídica, para utilizar da expressão do saudoso mestre, quando cogitamos do diálogo entre os dois microssistemas, merecem menções específicas.

No mesmo período da promulgação do Código Brasileiro de Defesa do Consumidor e nos anos que se seguiram, podemos mencionar leis que se integraram a esse microssistema.

Foi o caso do Estatuto da Criança e do Adolescente (Lei nº 8.069/90 de 13 de julho de 1990).

Neste, destacam-se os arts. 148, 201, 208 e, principalmente, no art. 224 que tem a seguinte redação, denotando a integração ao microssistema:

> Art. 224. Aplicam-se subsidiariamente, no que couber, as disposições da Lei n.º 7.347, de 24 de julho de 1985. [79]

Não é só. Também no denominado Estatuto da Cidade (Lei nº 10.257 de 10 de julho de 2001) que derrogou o art. 4º da Lei da Ação Civil Pública, acima referida, de acordo com seu art. 54,[80] incluindo a proteção à ordem urbanística como interesse transindividual.

---

[78] GOMES, Orlando. A agonia do Código Civil. *Revista de Direito Comparado Luso-brasileiro*, 1988, n. 07, pp. 01-09, p. 04.

[79] Cf. https://www.planalto.gov.br/ccivil_03/leis/l8069.htm

[80] Cf. https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm

No mesmo sentido, o denominado Estatuto do Idoso (Lei n° 10.741 de 1º de outubro de 2003) em seus arts. 74, inciso I e 79, parágrafo único e art. 93 que, igualmente, remete à Lei da Ação Civil Pública[81].

Mais recentemente, a Lei Brasileira de Inclusão (Estatuto da Pessoa Com Deficiência (Lei n° 13.146 de 6 de julho de 2015)que, expressamente prevê que medidas judiciais destinadas à proteção de interesses coletivos, difusos, individuais homogêneos e individuais indisponíveis da pessoa com deficiência poderão ser propostas pelo Ministério Público, pela Defensoria Pública, pela União, pelos Estados, pelos Municípios, pelo Distrito Federal, por associação constituída há mais de 1 (um) ano, nos termos da lei civil, por autarquia, por empresa pública e por fundação ou sociedade de economia mista que inclua, entre suas finalidades institucionais, a proteção dos interesses e a promoção de direitos da pessoa com deficiência.[82]

Nesse momento, torna-se possível identificar o diálogo criado entre o microssistema da tutela jurisidiconal coletiva e o microssistema do ambiente digital.

Para ressaltar o diálogo entre os microssistemas referidos, há que se destacar a Lei Geral de Proteção de Dados (Lei nº 13.709 de 14 de agosto de 2018), que menciona expressamente a possibilidade de tutela coletiva dos interesses e dos direitos dos titulares de dados.

Vejamos a redação de seu art. 22:

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva[83].

[81] Cf. https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm
[82] Cf. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm
[83]. Cf. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Obviamente, a título individual, a Lei Geral de Proteção de Dados está se referindo ao vigente Código de Processo Civil, Lei nº 13.105, de 16 de março de 2015, cuja estrutura é de índole individualista, como bem demonstra o seu art. 17 a exigir a comprovação da legitimidade ativa (pertinência subjetiva da demanda) e o interesse de agir, de cada qual que ajuíza uma demanda em juízo, a fim de tutelar seus próprios em individuais interesses

Adiante, no art. 52, a Lei Geral de Proteção de dados menciona que as sanções previstas na Lei não substituem as sanções previstas no referido Código de Defesa do Consumidor.

Convém destacar, também, o art. 42, §3º da LGPD, que dispõe sobre a possibilidade de tutela coletiva em sede de ação de reparação de danos coletivos.

Importante a transcirção de tal dispositivo, a fim de se demonstrar a relação que cria entre a Lei Geral de Proteção de dados e o micorssistema da tutela jurisdicional coletiva, anteriormente explorado (a correlação entre Lei da Ação Civil Pública e o Código de Defesa do Consumidor):

> "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de da- dos pessoais, é obrigado a repará-lo. (...)
>
> §3º. As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente;"[84]

Na primeira parte do desenvolvimento da existência do microssistema do ambiente digital, já tivemos a oportunidade de demonstrar que a Lei Geral de Proteção de Dados é o eixo desse sistema.

[84]. Cf https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Considerando que remete à legislação pertinente a disciplina da responsabilização coletiva da responsabilidade civil e que referida responsabilização se faz pelas normas do microssistema da tutela jurisdicional coletiva, podemos concluir que o microssistema do ambiente digital àquele microssistema se relaciona, constituindo um novo centro da experiência jurídica

Referências

GOMES, Orlando. A agonia do Código Civil. *Revista de Direito Comparado Luso-brasileiro*, 1988, n. 07, pp. 01-09, p. 04.

IRTI, Natalino. *L'età della decodificazione*. 4ª ed. Milano: Giuffrè, 1999.

VIGLIAR, Jose Marcelo Menezes. Tutela Jurisdicional Coletiva. 1ª Edição. São Paulo: Atlas, 1998.

A RESPONSABILIDADE POR DANOS PROVOCADOS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL À LUZ DO PROJETO DE LEI Nº 2338/2023.

NIVALDO SEBASTIÃO VÍCOLA

A RESPONSABILIDADE POR DANOS PROVOCADOS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL À LUZ DO PROJETO DE LEI Nº 2338/2023.

Introdução

O presente estudo tem por objetivo analisar a responsabilidade civil decorrente de danos provocados por sistemas de inteligência artificial, ou algoritmos inteligentes, como preferem alguns, à luz do Projeto de Lei nº 2338 de 2023 (PL 2338/2023), de iniciativa do Senador Rodrigo Pacheco (PSD/MG), em trâmite perante o Senado da República.

Embora seja específico o objeto deste estudo, ou seja, os danos provocados por sistemas de inteligência artificial (IA), parece-nos de fundamental importância tecer breves considerações sobre o instituto da Responsabilidade Civil, tanto em seu aspecto histórico, quanto em seu aspecto estrutural, uma vez que o dano é elemento essencial do referido instituto.

1. RESPONSABILIDADE CIVIL

1.1. Origem histórica

A responsabilidade civil é um desses institutos que, tendo entrado no universo jurídico por volta do século III a.C., jamais deixou de ocupar papel de

destaque. Dado que a liberdade de escolha (livre arbítrio) é própria do homem e o pano de fundo de suas relações socioeconômicas, a responsabilidade, invariavelmente, aparece como a consequência inexorável de tais escolhas, mormente quando, aos olhos do homem médio, probo e civilizado, referidas escolhas se apresentam como "más escolhas" (Vícola, 2021, p. 170).

Com Álvaro Villaça Azevedo (2011, p. 261) aprendemos que a palavra responsabilidade tem sua origem no verbo latino respondere, de *spondeo*, sendo concebida no período clássico do direito romano como uma obrigação de natureza contratual, verbal, cujo objetivo era vincular o devedor ao credor através da fórmula: *spondesne mihi dare Centum? Spondeo* u seja, prometes me dar um cento? Prometo).

Concebida originalmente como vingança privada, a responsabilidade, tida como o dever de indenizar o dano causado ilicitamente, tem sua origem legislativa na *Lex Aquilia (damnum iniuria datum)* que, a partir do sec. III a.C., irá estabelecer a necessidade de reparar o dano causado ilicitamente ao proprietário de uma coisa pela destruição ou deterioração desta (Vícola, 2021, p. 170).

Cumpre observar, também, o posicionamento majoritário de que entre os romanos do período clássico inexistia tanto a distinção que modernamente se faz entre responsabilidade penal e civil, quanto a proporcionalidade entre dano e prejuízo. Segundo Rogério Donnini (2009, p. 489), é na *Lex Aquilia de Damno* "que foram substituídas as penas fixas (indenização tarifária) por uma pena proporcional ao prejuízo causado".

Referida lei, que acabou se transformando em sinônimo de responsabilidade extracontratual (responsabilidade aquiliana), estabeleceu as bases da responsabilidade subjetiva (fundada na culpa) e serviu de paradigma para a codificação do século XIX, como são exemplos os Códigos: Francês de 1804, Italiano de 1865, Alemão de 1896 e o nosso Código Civil de 1916. (Vícola, 2021. p. 171)

Não nos olvidemos que a codificação civil iniciada na França em 1804 e que se espalhou rapidamente pela Europa, teve, como um de seus pilares, o ideário iluminista de liberdade. Portanto, o fato da responsabilidade puramente civil surgir apenas a partir daí, se justifica em vista da necessidade de estabelecer limites à liberdade, mormente quando o seu exercício causar dano a outrem. (Gilissen, 2001, p. 752)

É também a partir do final do século XIX que começa a surgir, na França, as primeiras teorias sustentando a responsabilidade sem culpa (responsabilidade objetiva) que, para alguns, representa a nova tendência no campo da responsabilidade civil e que, no futuro, fará desaparecer a responsabilidade subjetiva. O argumento central, para os defensores dessa ideia, é que a teoria da culpa, em virtude de sua manifesta subjetividade, vem encontrando cada vez mais dificuldade para tratar a multiplicidade de riscos propiciados pela vida moderna. (Vícola, 2021, p. 171)

Entre nós, não foi automático o salto da responsabilidade subjetiva para a objetiva, uma vez que tal passagem foi precedida pela culpa presumida, que tem como pressuposto o dever genérico de indenizar. Aliás, conforme ensina Flávio Tartuce (2011, p. 15), "o Código Civil de 1916 também tratava da responsabilidade objetiva ou sem culpa". Essa, lembra o citador autor, era a interpretação doutrinária "da responsabilidade civil decorrente do fato da coisa, constante dos arts. 1.519 e 1.520, parágrafo único, 1.528 e 1.529" do citado código.

No mesmo sentido é a posição de Paulo Luiz Lôbo Netto (1998, p. 159-165). Sustentando a posição intermediária da culpa presumida, atesta o citado autor que "constitui um avanço na tendência evolutiva que aponta para a necessidade de não se deixar o dano sem reparação, interessando menos a culpa de quem o causou e mais a imputar a alguém a responsabilidade pela indenização".

Vale observar, no entanto que, entre nós, a primazia da adoção da teoria objetiva foi do Código de Defesa do Consumidor (Lei nº 8.078/1990), tendo a mesma sido posteriormente encampada pelo Código Civil de 2002, que lhe deu a merecida abrangência.

1.2. Conceito

Por responsabilidade devemos entender a "aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros, em razão de ato do próprio imputado, de pessoa por quem ele responde, ou de fato de coisa ou animal sob sua guarda, ou, ainda, de simples imposição legal". (Azevedo, 2011, p. 244)

Ainda, segundo Azevedo (2011, p. 244), referido conceito é o mais aceito pela doutrina nacional, eis que ampara a ideia da responsabilidade subjetiva (quando cogita a existência do ato ilícito) e a responsabilidade objetiva, ou do risco.

Conforme definido no Considerando (1) do Anexo B da Proposta de Resolução de outubro de 2020 do Parlamento Europeu, o conceito de responsabilidade desempenha papel duplo em nosso cotidiano posto que, se por uma lado garante que uma pessoa que tenha sofrido prejuízos ou danos tenha o direito de exigir uma indenização à parte que é responsável por esses prejuízos ou danos, por outro,

> proporciona incentivos econômicos para que as pessoas evitem, desde logo, causar prejuízos ou danos. Qualquer quadro em matéria de responsabilidade deverá procurar incutir confiança na segurança, fiabilidade e coerência dos produtos e serviços, incluindo as tecnologias digitais emergentes, como a inteligência artificial (IA), a Internet das Coisas (IdC) ou a robótica, a fim de estabelecer um equilíbrio entre uma proteção eficaz das potenciais vítimas de danos ou prejuízos e, simultaneamente, prever uma margem de manobra suficiente para permitir o desenvolvimento de novas tecnologias, produtos ou serviços.

1.3. Elementos

Partindo do conceito acima transcrito e tomando por base a norma do Art. 186 de nosso Código Civil, combinada com aquela estipulada no *caput* do Art. 927 do mesmo diploma legal, temos que para a caracterização da responsabilidade civil e, por conseguinte, do dever de indenizar, devem estar presentes os seguintes elementos: (i) ação ou omissão voluntária; (ii) dano; (iii) nexo causal; e (iv) culpa. (Vicola, 2021, p. 173)

Sem a intenção de nos aprofundarmos no assunto, eis que fugiria do propósito deste estudo, mas, tecendo algumas breves considerações a respeito dos elementos constitutivos da responsabilidade civil supratranscritos, temos:

a) Ação ou omissão voluntária: nas palavras de Francisco Vieira Lima Neto (2006, p.242), os adeptos da teoria subjetiva sustentam ser necessário que a ação

> tenha sido culposa, vale dizer, o ato praticado deve possuir uma qualificação especial que consiste, em termos subjetivos, *na possibilidade do agente conhecer previamente o dever violado e mesmo assim decidir praticar o ato que poderia viola-lo, seja porque pretendia causar o prejuízo, seja porque assumiu esse risco, embora não desejasse que o dano ocorresse*: e na possibilidade de cumprir esse dever, de observa-lo; vale dizer, o agente possui forças suficientes para cumprir o dever jurídico que acabou descumprindo, não há, portanto, culpa, se o agente era inimputável.

b) Nexo de causalidade: segundo a doutrina majoritária, é o aspecto da responsabilidade civil que deve merecer maior atenção da doutrina e da jurisprudência.

Para Sérgio Cavalieri Filho (2010, p. 50), "em sede de responsabilidade civil, nem todas as condições que concorrem para o resultado são equivalentes". Dessarte, preceitua o autor que deve ser considerada somente aquela condição

> [...] que foi a mais adequada a produzir concretamente o resultado"; sendo, ainda necessário, no caso concreto, que,

> "além de se indagar se uma determinada condição concorreu concretamente para o evento é ainda preciso apurar se, em abstrato, ela era adequada a produzir aquele efeito. Entre duas ou mais circunstâncias que concretamente concorreram para a produção do resultado, causa adequada será aquela que teve interferência decisiva.

Embora pacífico o entendimento, também exarado na lição de Maria Helena Diniz (2014, p. 611), de que a responsabilidade civil não pode existir sem a relação de causalidade e a conduta ilícita do agente (ação ou omissão) é fato, conforme leciona Rogério Donnini (2009, p. 491), que tal pressuposto não é absoluto posto ter sofrido alguma relativização, como ocorre nos casos de danos causados ao meio ambiente. Lembra o mesmo autor que, "sob o argumento de que a obrigação é *propter rem*", o proprietário responde independentemente da prova da relação direta entre a ação ou omissão e o dano.

Discorrendo sobre os sistemas de inteligência artificial, o Parlamento Europeu, em especial no Considerando (3) do Anexo B. Texto da Proposta Requerida, da Resolução de outubro de 2020, estabelece que a identificação do nexo de causalidade se torna, muitas vezes, um desafio para os quadros de responsabilidade existentes. Nos termos da citada normativa, a utilização de sistemas de IA em nosso cotidiano conduzirá a situações

> [...] em que a sua opacidade (elemento de caixa negra) e a série de intervenientes no seu ciclo de vida tornem extremamente dispendioso, ou mesmo impossível, identificar quem exercia o controle do risco de utilização do sistema de IA em questão ou qual foi o código ou entrada que provocou a operação danosa. Essa dificuldade é agravada pela conectividade entre um sistema de IA e outros sistemas de IA e sem IA, pela sua dependência de dados externos, pela sua vulnerabilidade a violações da cibersegurança e ainda pela crescente autonomia dos sistemas de IA desencadeados pelas capacidades de aprendizagem automática e aprendizagem profunda. Para além destas características complexas e potenciais vulnerabilidades, os sistemas de IA também podem ser utilizados para causar danos graves – como comprometer a dignidade humana e os valores e

> liberdades europeus – através da localização de pessoas contra a sua vontade, da introdução de sistemas de crédito social, de decisões enviesadas em matérias relacionadas com seguros de doença, concessão de crédito, decisões judiciais, recrutamento ou emprego, ou da construção de sistemas de armas letais autónomas. (Parlamento Europeu, 2020 – *on-line*).

c) Dano: do latim, *damnum,* é frequentemente traduzido por prejuízo e, conforme a doutrina tradicional, ao lado da culpa representa o segundo elemento mais importante entre aqueles que formam a estrutura da responsabilidade civil, sendo pacífico o entendimento de que, inexistindo o dano, inexiste o dever de indenizar. (Vícola, 2021, p. 178)

Segundo Flávio Tartuce (2011, p. 92), por dano "deve-se entender a presença de um prejuízo real, um mal, um detrimento, uma perda a alguém". Para o mesmo autor, citando Aguiar Dias, "a concepção de dano como prejuízo é pressuposto do dever de indenizar".

No mesmo sentido é a lição de John Gilissen (2001, p. 750), para quem, tanto o direito bizantino, quanto o Código de Napoleão de 1804, estabelecem a obrigação de reparar o dano, ou prejuízo causado. No direito bizantino encontrarmos que a "obrigação de reparar o prejuízo resulta da responsabilidade daquele que cometeu o ato culposo", enquanto o Art. 1.382 do Código de Napoleão estipula que "qualquer ação humana que cause a outrem um *prejuízo obriga a reparação deste por parte daquele por cuja culpa tal ação aconteceu*". (grifamos)

A doutrina moderna tem estabelecido a distinção entre dano patrimonial (modalidade mais tradicional de dano), ou seja, aquele que atinge diretamente o patrimônio do lesado e necessita ser provado, eis que, nessa modalidade não se admite o dano hipotético; e dano moral, este, de caráter extrapatrimonial, é mais difícil de conceituação, posto que diretamente relacionado aos princípios da

dignidade da pessoa humana e da justiça social, vinculado aos direitos da personalidade, portanto.

Nas palavras de Flávio Tartuce (2011, p. 95), temos que o tema dano moral é relativamente novo entre nós eis que

> a possibilidade de reparação de danos imateriais ou extrapatrimoniais se consolidou a partir da Constituição Federal de 1988. Na codificação revogada, o art. 159 do Código Civil de 1916 reconhecia a possibilidade de reparação de danos, sem, contudo, fazer menção expressa ao dano extrapatrimonial. Contudo, Clóvis Beviláqua, principal idealizador da codificação anterior, ensinava que a reparação moral era implícita em tal dispositivo. Entretanto, na vigência daquele Código, a reparação de danos morais não era aceita com unanimidade, principalmente em sede jurisprudencial.

Nesse diapasão, merece destaque o dano moral *in re ipsa*, classificado como presumido e que, em consequência, não necessita ser provado por quem o alega. Para Sérgio Cavalieri Filho (2010, p. 101), quando estamos diante de um dano moral objetivo (*in re ipsa*), não há necessidade de provar o abalo psíquico sofrido. Basta que quem o alega demonstre a ofensa (*ipso facto*) e estará demonstrado o dano moral que é presumido a partir das regras de experiência comum.

Basta, portanto, ao lesado, oferecer prova da ação, uma vez que o dano existe *in re ipsa*. É oportuno observar, no entanto, que, nos termos do Enunciado 159 do Conselho da Justiça Federal (CJF), o dano moral, assim compreendido todo dano extrapatrimonial, não se caracteriza quando há mero aborrecimento inerente a prejuízo material. A doutrina tem se posicionado majoritariamente a favor desse entendimento porquanto encontramos, em nossos tribunais, incontáveis exemplos de supostos danos morais que, em realidade, não passam de meros aborrecimentos inerentes a prejuízos materiais. Entre tais exemplos podem ser citados os casos de acidentes envolvendo automóveis novos; furtos de estojos de maquiagem e

assemelhados; presença de insetos no interior de garrafas d´água transparentes, fechadas, entre outros.

A referência ao disposto no Enunciado 159 do CJF supramencionado ganha importância quando observamos, como veremos adiante, que a tendência legislativa é de classificar como objetiva a responsabilidade, tanto do fornecedor, quanto do operador, quando se tratar de dano provocado por sistemas de Inteligência Artificial de alto risco ou de risco excessivo.

d) Culpa: diversamente do que ocorre com o dano, o conceito de culpa não é unívoco, posto que sua definição vai depender da posição adotada (teoria subjetiva ou teoria objetiva). Para os adeptos da teoria subjetiva, a culpa, além de ser princípio constitutivo da responsabilidade (conforme estabelecem os artigos 186 e 927 de nosso Código Civil), é, segundo prevê a norma do parágrafo único do Art. 944 do referido Código, elemento redutor da indenização. Para os defensores da teoria objetiva, a culpa é a violação do dever estipulado na lei ou no contrato.

Portanto, seja em virtude de determinação legal, seja em virtude do exercício de uma atividade que, por sua própria natureza, implique em riscos, a existência de dano acarreta a responsabilidade civil e o dever de indenizar, independentemente de culpa, conforme estipula o parágrafo único do Art. 927 do Código Civil em vigor, nos termos seguintes: "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem". (Vícola, 2021, p. 174)

Por atividade normalmente desenvolvida pelo autor do dano entende-se aquela desempenhada de modo habitual, sem o caráter de eventual ou esporádica, portanto.

O risco, por sua vez, costuma ser classificado em: a) risco criado, assim entendido aquele não advindo necessariamente de uma atividade coordenada,

como é exemplo um vaso atirado ou caído da sacada de um edifício; b) risco proveito (que é a adotada pelo nosso Código de Defesa do Consumidor em relação aos fornecedores de produtos e serviços), aquele que traz vantagem para quem o cria, em desfavor de outrem; c) risco profissional, aquele relacionado à atividade desenvolvida pelo agente de forma habitual, como é exemplo o dano causado pelo empregador ou seu empregado a terceiros e/ou prepostos; d) risco integral, aquele em que a responsabilidade é objetiva e não admite excludente, como ocorre nos casos de danos ao meio ambiente; e e) risco dependência, que, segundo José Fernando Simão (2009, p. 299), aplica-se nas hipóteses de dano causado pelo incapaz, conforme prevê a norma do Art. 928 do Código Civil. (Tartuce, 2011, p. 386-387).

2. INTELIGÊNCIA ARTIFICIAL

2.1. Conceito

Tomemos aqui aquela que nos parece ser a definição de Inteligência Artificial mais apropriada, tendo em vista que, embora não faça referência direta ao binômio pensar/agir, comum às definições de IA, encontra perfeita sintonia com o referido binômio. Tal definição é aquela proposta por Selmer Bringsjord e Naveen Sundar Govindarajulu (2020 – *on-line)* sustentando que, por IA deve-se entender "o campo dedicado à construção de animais artificiais (ou pelo menos criaturas artificiais que – em contextos adequados – *parecem* ser animais) e, para muitos, pessoas artificiais (ou pelo menos criaturas artificiais que – em contextos adequados – *parecem* ser pessoas)[85].

A definição de Selmer Bringsjord e Naveen Sundar Govindarajulu acima transcrita, além de ser aquela que, a nosso ver melhor representa o atual estágio

[85] Tradução nossa. No original: "Artificial intelligence (AI) is the field devoted to building artificial animals (or at least artificial creatures that – in suitable contexts – ***appear*** to be animals) and, for many, artificial persons (or at least artificial creatures that – in suitable contexts – ***appear*** to be persons)"

de desenvolvimento da IA, torna-se ainda mais esclarecedora quando associamos a ela a nota número um[86] apresentada pelos mesmos autores, dando conta de que

> [...] alguns pesquisadores e/ou engenheiros de IA certamente não se verão empenhados em construir animais e/ou pessoas. No entanto, se eles estão operando sob qualquer uma das contas ortodoxas (algumas das quais são exploradas abaixo) de quais artefatos a pesquisa e a engenharia de IA devem produzir, o resultado final é que os artefatos que se destinam a ser construídos são precisamente considerados artificiais, *correlatos dos únicos seres inteligentes não artificiais que a raça humana foi capaz de localizar até agora: a saber, animais da variedade não humana e nós.* É verdade, porém, que alguns aspiram construir criaturas artificiais que excedem em muito os poderes cognitivos fornecidos pela natureza; discutiremos esse problema separadamente, abaixo (grifamos).

2.2. A responsabilidade por danos provocados por sistemas de inteligência artificial

Apesar do objetivo específico deste estudo ser o tratamento dado pelo Projeto de Lei nº 2338/2023, em trâmite perante o Congresso Nacional, aos sistemas de IA, é importante lembrar o pioneirismo do Parlamento Europeu quanto à regulamentação da matéria.

Tanto é verdade que, desde fevereiro de 2017, quando a Comissão de Assuntos Jurídicos daquele Parlamento adotou o relatório da deputada de Luxemburgo, Mady Delvaux-Stehres (2017 – *on-line*), colocando o tema em relevo e realçando a necessidade da adoção de regras no sentido de disciplinar o uso da inteligência artificial e das tecnologias conexas, algumas questões ético-jurídicas compreendendo os algoritmos inteligentes e, na grande maioria delas, em especial

[86] Tradução nossa. No original: "The pair of parentheticals here are indispensable, and worth noting, since some AI researchers and/or engineers will surely not see themselves as striving to build animals and/or persons. Nonetheless, if they are operating under any of the orthodox accounts (some of which are explored below) of what artifacts AI research and engineering is to produce, the bottom line is that the artifacts that are intended to be built are accurately said to be artificial correlates of the only non-artificial intelligent beings the human race has been able to locate so far: viz., animals of the non-human variety, and us. It's true, however, that some aspire to build artificial creatures that greatly exceed the cognitive powers of what nature has supplied; we discuss this issue separately, below".

naquelas que envolvem risco elevado, aparece o tema da responsabilidade civil. Cumpre observar, por oportuno, que em outubro de 2020, o Parlamento Europeu aprovou, "uma resolução que contém recomendações à citada Comissão de Assuntos Jurídicos sobre a necessidade de um regime de responsabilidade civil para a inteligência artificial." (2021 – *on-line)*

Não nos olvidemos, ainda, que a supracitada resolução do Parlamento Europeu foi ratificada, em sua quase totalidade, no início de 2021. Em meados de 2023, no entanto, o texto da referida Resolução sofreu algumas alterações, as quais, a nosso ver, tornaram mais amenos alguns de seus preceitos, pugnando, porém, pelo estabelecimento de regras baseadas no risco e, consequentemente, no estabelecimento de obrigações para os fornecedores e usuários de sistemas de IA. Nessa última revisão, ocorrida em junho de 2023, o Parlamento Europeu (2023 – *on-line)* recomendou cuidado, tanto para os fornecedores, como para aqueles que utilizam sistemas de IA, em função do nível de risco que tais sistemas podem oferecer. Por consequência,

> os sistemas de IA com um nível de risco inaceitável para a segurança das pessoas serão proibidos, como os utilizados para classificação das pessoas com base no seu comportamento social ou nas suas características pessoais. Os eurodeputados alargaram a lista de modo a incluir proibições de utilizações intrusivas e discriminatórias da IA, tais como: i) sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público; ii) sistemas de identificação biométrica à distância em diferido, com a única exceção para a repressão de crimes graves por autoridades responsáveis pela aplicação da lei e apenas após autorização judicial; iii) sistemas de categorização biométrica que utilizem características sensíveis (por exemplo, gênero, raça, etnia, estatuto de cidadania, religião, orientação política); iv) sistemas de policiamento preditivo (baseados na definição de perfis, localização ou comportamento criminoso passado); v) sistemas de reconhecimento de emoções na aplicação da lei, na gestão das fronteiras, no local de trabalho e nos estabelecimentos de ensino; e vi) remoção não direcionada de imagens faciais da Internet ou de filmagens

> de video vigilância (circuito fechado) para criar bases de dados de reconhecimento facial (violação dos direitos humanos e do direito à privacidade).

Sob essa mesma perspectiva e considerando a utilização cada vez mais crescente da tecnologia no cotidiano das pessoas e das instituições, Eduardo Magrani (2019 – *on-line*) aponta para importantes reflexões éticas e jurídicas que devem permear a discussão em torno dos algoritmos inteligentes. Entre as questões abordadas pelo citado autor, merece especial destaque aquela relativa ao "regime de responsabilidade legal que devemos adotar por danos decorrentes da inteligência artificial (IA), cada vez mais avançada", eis que, segundo o mesmo autor, a capacidade de acumular experiência e aprender

> [...] com o processamento massivo de dados, juntamente com a capacidade de agir de forma independente e fazer escolhas de forma autônoma, podem ser consideradas pré-condições para a responsabilidade legal. No entanto, uma vez que a inteligência artificial não é reconhecida hoje como um sujeito de lei, ela não pode ser responsabilizada individualmente pelos danos potenciais que possa causar.

Nesse sentido, conforme ensinam Marco Bassini, Laura Liguori e Oreste Pollicino (2015, p. 341) tem trilhado até aqui a União Europeia. Pelo fato de a normativa ali vigente não contemplar normas específicas sobre a responsabilidade dos robôs, trata-os como produtos. Para referidos autores:

> O quadro legislativo atual não contempla disposições normativas para essa finalidade no que diz respeito aos robôs, ou mais amplamente às inteligências artificiais, sob o perfil de responsabilidade aplicável. A ausência de tais normas dá-se pelo fato de que até agora foram sempre aplicadas as regras e as normas desenvolvidas para os produtos. Portanto, nunca se colocou como exigência prever normas específicas de responsabilidade e da modalidade de ressarcimento dos respectivos danos.[87]

[87] Tradução nossa. No original: "Il quadro legislativo attuale non contempla delle disposizioni normative *ad hoc* per quanto riguarda i robot e, più in generale, le intelligenze artificiali, sotto il profilo del regime di responsabilità applicabile. L'assenza di tali norme è dovuta al fato che, finora, si sono sempre

Situação análoga, entre nós, ao menos enquanto não dispúnhamos de legislação específica regulamentando as hipóteses de responsabilidade por danos causados pelos sistemas de IA, seria aquela prevista na norma do art. 931 do Código Civil de 2002, que trata da responsabilidade das empresas e empresários individuais, combinada com a norma do art. 12 do Código de Defesa do Consumidor, que estabelece a respeito da responsabilidade objetiva do fabricante, do produtor, do construtor e do importador pelos danos causados aos consumidores, ou seja, responsabilidade do produto. (Vícola, 2021, p. 184-185)

Com o advento do Projeto de Lei nº 2338/2023 (PL 2338/2023), no entanto, por força da redação de seu Art. 27, a responsabilidade tanto do fornecedor, quanto do operador, quando se tratar de dano provocado por sistemas de IA de alto risco ou de risco excessivo, será objetiva. Para os demais sistemas -, embora a redação do §2º do referido Art. 27 não explicite, entendemos tratar-se de sistemas de risco limitado -, onde presume-se a culpa do causador do dano, adotando-se, no caso, a inversão do ônus da prova.

Vale, por oportuno, observar que, pela redação do Art. 29 do referido PL nº 2338/2023, as hipóteses de

> responsabilização civil decorrentes de danos causados por sistemas de inteligência artificial no âmbito das relações de consumo permanecem sujeitas às regras previstas na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), sem prejuízo da aplicação das demais normas desta Lei.

Também os Estados Unidos da América seguem regra semelhante. Conforme sustentam Marco Bassini, Laura Liguori e Oreste Pollicino (2015, p. 348)[88] "nos casos em que seja necessário determinar a responsabilidade de um robô, são

applicate le regole e l enorme sviluppate per i prodotti. Non si è mai dunque posta l'esigenza di prevedere dele forme specifiche di responsabilità – e di modalità di risarcimento dei danni connesse".

[88] Tradução nossa. No original: "Anche negli Stati Uniti l enorme al momento applicabili – e applicate – nei casi in cuisia necessário determinar ela responsabilità d um robot sono sempre quelle dela responsabilità da prodotto ('product liability law')".

sempre aplicáveis as normas relacionadas à responsabilidade do produto ('product liability law')". (Vícola, 2021, p. 185)

Se é fato, como reconheceu o Parlamento Europeu no item 4 do "Anexo B – Texto da proposta solicitada. Proposta para um regulamento do parlamento europeu e do conselho sobre responsabilidade pela operação de sistemas de Inteligência Artificial" (2020 – *on-line*), que as vantagens obtidas com a implantação de sistemas de IA são superiores às desvantagens, não se pode olvidar, também, que, nos termos fixados pelo mesmo Parlamento – item 3 do referido Anexo B – a ascensão da IA constitui um desafio significativo para os quadros de responsabilidade existentes, uma vez que a utilização de sistemas de IA em nosso cotidiano

> [...] levará a situações em que sua opacidade (elemento de "caixa-preta") e a multidão de atores que intervêm em seu ciclo de vida tornam extremamente caro ou mesmo impossível identificar quem estava no controle do risco de usar o sistema AI em questão ou qual código ou entrada causou a operação prejudicial. Essa dificuldade é agravada pela conectividade entre um sistema de IA e outros sistemas de IA e não sistemas de IA, por sua dependência de dados externos, por sua vulnerabilidade a violações de segurança cibernética, bem como pela crescente autonomia dos sistemas de IA acionados por recursos de aprendizado de máquina e aprendizado profundo. Além desses recursos complexos e vulnerabilidades potenciais, valores e liberdades, rastreando os indivíduos contra sua vontade, introduzindo sistemas de crédito social, tomando decisões tendenciosas em matéria de seguro-saúde, concessão de crédito, ordens judiciais, recrutamento ou emprego ou construindo sistemas de armas autônomas letais.

Com o intuito de equacionar tal desafio, o Parlamento Europeu reconheceu que, embora a Diretiva de Responsabilidade do Produto tenha sido eficaz por mais de três décadas, é necessária a revisão de seu texto, visando adequá-lo aos novos desafios jurídicos provocados pela IA. Por conseguinte, sustenta a necessidade de, em prol de "garantir a máxima segurança jurídica em toda a cadeia de

responsabilidade, incluindo produtor, operador, lesados e quaisquer outros terceiros, de forma a responder aos novos desafios jurídicos criados pelo desenvolvimento dos sistemas de inteligência artificial (IA)". (Vícola, 2021, p. 187)

É mandatório, contudo, que esse enfrentamento legislativo, além da necessária prudência no sentido de conciliar a proteção dos cidadãos, sem criar entraves ou retrocessos, nem desencorajar o desenvolvimento tecnológico em curso, considere o grau assimétrico de risco de que os sistemas de IA são capazes de proporcionar à sociedade. Dessarte, o Parlamento Europeu que, há bem pouco tempo sugeria que se levassem em conta, tanto no ambiente físico quanto no virtual, duas espécies de sistemas de IA, ou seja, aquelas que oferecem baixo risco e aquelas que representam risco elevado, em 2023, acrescentou a essa lista duas novas categorias: aquelas espécies que representam riscos inaceitáveis à sociedade humana e, em vista disso, devem ser proibidas e aquelas denominadas de sistemas generativos, que podem ser desenvolvidas, porém, segundo critérios pré-definidos.

Cumpre observar ainda que tanto para os sistemas de IA de alto risco quanto para os de baixo risco "não são considerados responsáveis pelos prejuízos ou danos se estes tiverem sido causados por motivos de força maior". Não poderá o operador, no entanto, "furtar-se à sua responsabilidade, alegando que os prejuízos ou danos foram causados por uma atividade, um dispositivo ou um processo autônomo baseado no seu sistema de IA". (Vícola, 2021, p. 189)

É importante e necessário frisar que, considerando a posição do Parlamento Europeu, de junho de 2023, retro referenciada, no sentido de realizar "negociação sobre o Regulamento de Inteligência Artificial (IA), em antecipação às conversações com os Estados-Membros da UE sobre a forma final da lei" a ser brevemente promulgada, parece óbvio supor que as referências a 'sistemas de alto risco', contidas nos itens das Resoluções de 2020 e 2021 supratranscritos, serão atualizadas para 'sistemas de risco elevado' ou, a depender do contexto, para

‘sistemas de risco inaceitável’, de igual modo, mantendo o mesmo raciocínio, as referências a ‘sistemas de baixo risco’ passam para ‘sistemas de risco limitado’.

Relembremos aqui a posição de Alexandre Simões que, ao comentar a proposta de regulamento de IA, então em trâmite perante o Congresso Nacional Brasileiro – PL n.º 21/2020 –, sustentava ser a responsabilidade civil o grande dilema que está a permear o debate em situações que resultem em acidentes envolvendo automóveis autônomos, por exemplo. Quem deve ser responsabilizado: “o fabricante do carro, o do *software*, ambos, ou nenhum deles”? Para o citado doutrinador, entretanto, é positivo o fato de o supramencionado Projeto de Lei brasileiro, à época em trâmite perante a Câmara dos Deputados, prever “a necessidade de apontar uma instituição a ser responsabilizada em caso de falha. Talvez, em alguns casos, possa ser criada uma anotação de responsabilidade técnica, como se usa na engenharia, que permita associar uma pessoa aquele sistema em particular”. (Vícola, 2021, p. 190)

A nosso ver, no entanto, as disposições contidas nos artigos 27, 28 e 29 do PL nº 2338/2023, superam essa questão posto que, tendo adotado a teoria do risco criado, trata como objetiva a responsabilidade, tanto do fornecedor, quanto do operador, quando o dano provocado advier de sistemas de IA de alto risco ou de risco excessivo. Por sua vez, para os danos provocados por sistemas de baixo risco, há a presunção de culpa do causador do dano, adotando-se, no caso, a inversão do ônus da prova.

Seguindo aquela que parece ser a tendência internacionalmente adotada, para aquelas hipóteses de danos provados por sistemas de IA no âmbito das relações de consumo, reza o Art. 29 do referido PL nº 2338/2023, que a responsabilização civil seguirá as normas previstas no Código de Defesa do Consumidor (Lei nº 8.078/1990).

CONSIDERAÇÕES FINAIS

O instituto da responsabilidade civil, desde a sua inserção no cenário romano do século III a.C., até nossos dias, nunca deixou de ocupar lugar de destaque. Seja em virtude do caráter patrimonial, ou extrapatrimonial do bem que se quer proteger, é fato, desde os primórdios, que aquele que causa dano, deve reparar.

Os movimentos legislativos iniciados na França, no início do século XIX, e que se espalharam pelo mundo, em especial pelos países de tradição romana, foram estruturados no sentido de amparar a regra acima, ou seja, da necessidade de reparar o dano causado ilicitamente ao proprietário de uma coisa pela destruição ou deterioração desta.

Concebida originalmente como responsabilidade de natureza contatual, foi, como vimos, se transformando em sinônimo de responsabilidade extracontratual (responsabilidade aquiliana), que serviu de base para a codificação civil do século XIX e de boa parte do século XX, até que as relações socioeconômicas originadas pela denominada Sociedade da Informação (fenômeno observado a partir da segunda metade do século XX), que têm no dinamismo e velocidade da informação seu elemento nuclear, passaram a exigir novas regras legislativas, as quais, no campo da responsabilidade civil, implementaram a responsabilidade objetiva.

É fato também, que a Sociedade da Informação, pautada pelo desenvolvimento da informática, em especial da internet e mais recentemente da Inteligência Artificial, criaram um Ambiente Digital que está a exigir novos contornos legislativos para que, ao lado da codificação tradicional, amparem as novas relações sociais e econômicas surgidas em virtude dele.

Dentre essas novas leis esparsas, que compõem um verdadeiro microssistema jurídico desse Ambiente Digital, certamente estará um 'marco civil' da Inteligência Artificial. Ações nesse sentido, como tivemos oportunidade de

analisar, têm sido verificadas no cenário europeu, desde 2017. Entre nós, tal movimento legislativo foi iniciado em 2020, com o PL 21/2020 e, mais recentemente, com a proposta do PL 2338/2023, de autoria do Senador Rodrigo Pacheco, em trâmite no Senado Federal.

Que os sistemas de inteligência artificial implementaram uma nova e importante realidade socioeconômica, é inegável. O que se está a perquirir é pelos limites ético-jurídicos desses novos sistemas e, no caso do objeto desse estudo, pelos riscos efetivamente apresentados por eles e, consequentemente, pela atribuição das responsabilidades pelos eventuais danos, se e quando ocasionados. A questão está aberta e, certamente, demanda, como de fato demandará, acaloradas discussões.

REFERÊNCIAS BIBLIOGRÁFICAS

AZEVEDO, Álvaro Villaça. Teoria geral das obrigações e responsabilidade civil. 12 ed. São Paulo: Atlas, 2011.

BASSINI, Marco; LIGUORI, Laura; POLLICINO, Oreste. Sistemi di Intelligenza artificiale, responsabilità e accountability. Verso nouvi paradigmi? *In*: PIZZETTI, Franco (coord.). *Intelligenza artificale, protezione dei dati personali e regolazione*. Torino: G. Giappichelli, 2015. p. 333-371.

BRASIL. Código Civil: Lei n.º 10.406, de 10 de janeiro de 2002. 7. ed. São Paulo: Manole, 2021.

BRASIL. Constituição Federal de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 out. 2023.

BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 out. 2023.

BRINGSJORD, Selmer; GOVINDARAJULU, Naveen Sundar. Artificial Intelligence. *The Stanford Encyclopedia of Philosophy* (Summer 2020 Edition). Edward N. Zalta (Ed.).

Disponível em: https://plato.stanford.edu/archives/sum2020 / entradas / inteligência artificial /. Acesso em: 13 ago. 2020.

CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 9 ed., São Paulo: Malheiros, 2010.

DINIZ, Maria Helena. Curso de direito civil brasileiro, volume 1: teoria geral do direito civil. 31. ed., São Paulo, Saraiva, 2014.

DONNINI, Rogério. Prevenção de danos e a extensão do princípio neminem laedere. In Responsabilidade civil: estudos em homenagem ao professor Rui Geraldo Camargo Viana. Rosa Maria de Andrade Nery e Rogério Donnini, Coord., São Paulo: RT, 2009, p. 483-503.

GILISSEN, John. Introdução histórica ao direito. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2001.

LIMA NETO, Francisco Vieira. Ato antijurídico e responsabilidade civil aquiliana – crítica à luz do novo código civil. In Introdução crítica ao código civil. Lucas Abreu Barroso, Org., Rio de Janeiro: Forense, 2006, p. 235-268.

LÔBO, Paulo Luiz Netto. Responsabilidade civil dos profissionais liberais e o ônus da prova. Revista de Direito do Consumidor, São Paulo, n. 26, p. 159-165, abr./jun. 1998.

MAGRANI, Eduardo. New perspectives on ethics and the laws of artificial intelligence. Internet Policy Review, v. 8, n. 3, 2019. Disponível em: https://doi.org/10.14763/2019.3.1420. Acesso em: 20 maio 2021.

NOGUEIRA, Pablo. Projeto de marco legal da IA no Brasil é pouco consistente e pode ser inútil, dizem especialistas. Disponível em: https://jornal.unesp.br/2021/07/29/projeto-de-marco-legal-da-ia-no-brasil-e-pouco-consistente-e-pode-ser-inutil-dizem-especialistas/. Acesso em: 31 ago. 2021.

PARLAMENTO EUROPEU. Regime de responsabilidade civil para a inteligência artificial. Disponível em: https://oeil.secure. europarl.europa.eu/oeil/popups/summary.do?id=1636987&t=e&l=en. Acesso em: 25 ago. 2021.

RESOLUÇÃO do Parlamento Europeu, de 20 de outubro de 2020. Anexo B. Texto da proposta solicitada. Proposta para um regulamento do parlamento europeu e do conselho sobre responsabilidade pela operação de sistemas de inteligência artificial.

Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html#title3. Acesso em: 21 ago. 2021.

SIMÃO, José Fernando. Fundamentos da responsabilidade civil. A responsabilidade do incapaz. In Responsabilidade civil: estudos em homenagem ao professor Rui Geraldo Camargo Viana. Rosa Maria de Andrade Nery e Rogério Donnini, Coord., São Paulo: RT, 2009, p. 285-300.

TARTUCE, Flávio. Responsabilidade civil objetiva e risco. A teoria do risco concorrente. São Paulo: Editora Método, 2011.

VICOLA. Nivaldo Sebastião. Personalidade Eletrônica na Teoria Geral do Direito Civil. Tese (Doutorado em Direito). Faculdade de Direito da Universidade de São Paulo, São Paulo, 2021.

http://professorflaviotartuce.blogspot.com.br/2012/06/artigo-de-jose-fernando-simao-sobre.html> .Acesso em: 6 mai. 2018.

https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1636987&t=e&l=en. Acesso em: 25 ago. 2021.

https://www.europarl.europa.eu/news/pt/press-room/20230609IPR96212/parlamento-negoceia-primeiras-regras-para-inteligencia-artificial-mais-segura. Acesso em: 25 jul. 2023.

ADMINISTRAÇÃO PÚBLICA NO MICROSSISTEMA JURÍDICO DO AMBIENTE DIGITAL

Tiago Cappi Janini

Introdução

A partir da década de 1990 um novo mundo começa a tomar forma, apoiado na mercantilização da internet e na revolução das tecnologias da informação. Tem-se uma profunda ruptura que impacta as relações sociais. O aparecimento dessas tecnologias conduz a uma digitalização da vida humana e lança novos parâmetros para os conflitos sociais que afloram mais complexos.

Essa revolução tecnologia carrega, assim como as anteriores, a desconstrução de paradigmas consolidados, buscando uma reavaliação e reconstrução do contexto científico e social. No cenário atual, a comodificação da informação transforma a sociedade em suas interações econômicas, políticas, científicas, sociais e jurídicas.

O direito, como parte fundamental da arquitetura da sociedade moderna, sofre interferências dessa ordem digital indeterminável, com irritações inexistentes há pouco tempo. Novas condutas sociais digitalizadas exigem uma resposta do ordenamento jurídico acerca de seus conflitos. Os tradicionais institutos jurídicos têm cada vez mais dificuldade em desempenhar o seu papel de organizador social. A impressionante velocidade do contínuo progresso tecnológico não é seguida de perto pelo direito. Eis a dificuldade do direito moderno: lidar com a complexidade social decorrente do advento de novas tecnologias computacionais, da informação e da comunicação.

Esses reflexos atingem não apenas as relações entre particulares. O Estado tem interagido, cada vez mais, com os novos aparatos e sistemas tecnológicos. O aparecimento de uma Administração Pública Digital gera uma série de dúvidas relevantes que tensionam o sistema jurídico, que precisa oferecer uma conceptualização adequada para os anseios apresentados pela Sociedade da Informação.

As mudanças sociais conduzidas pelas tecnologias acarretam alterações no contexto sociojurídico que implicam em uma movimentação das estruturas jurídicas. Aos problemas socais, políticos e econômicos oriundos das relações no ciberespaço o direito começa a fornecer respostas na forma de leis e jurisprudência. Pensar na construção de uma organização jurídica desse "novo" direito é uma tarefa árdua aos cientistas do direito, que envolve investigação, análise, catalogação e interpretação de todo tratamento jurídico das relações sociais que se sucedem dentro desse ambiente digital, abrangendo o privado e o público.

A proposta doutrinária de construção de um microssistema jurídico do ambiente digital tem o mérito de buscar preencher esse vácuo jurídico, voltando as atenções não apenas para a proteção de dados pessoais digitais, mas também para todas as espécies de relações sociais ciberespaciais. O microssistema jurídico do ambiente digital, em uma acepção ampla, se preocupa em proporcionar uma estrutura legal confiável, eficiente e legítima, com principiologia e os institutos próprios que o atual contexto sociojurídico reivindica, oferecendo respostas às demandas públicas e privadas da Sociedade da Informação.

Há de ficar claro que a ruptura causada pela revolução das tecnologias da informação atinge as ordens sociais privadas e públicas. A dinâmica da sociedade digital exige um reposicionamento de todos os ramos didáticos do direito. A interação da Administração Pública com as novas tecnologias acarreta uma concepção do direito público a partir desse paradigma transformador da Sociedade da Informação.

Essa inafastável digitalização das condutas administrativas implica uma inevitável regulamentação da atuação do Poder Público no ambiente digital. Nesse ponto, tem importância ressaltar que o microssistema jurídico do ambiente digital engloba as relações jurídicas em que figura o Estado em um de seus polos.

Pretende-se, desse modo, apresentar a aplicabilidade do microssistema jurídico do ambiente digital às relações jurídicas que envolvem a Administração Pública concretizadas no ciberespaço.

1 A Administração Pública controladora de dados

A revolução provocada pelos impactos da tecnologia na sociedade constrói um novo ambiente social com enfoque na vida e nas relações digitais. Não só o privado opera no contexto digital. A figura do Estado está presente nessa realidade virtual, tanto em suas atividades internas quanto no seu relacionamento com os cidadãos. O Poder Público presta serviços públicos, direciona políticas públicas, realiza atos administrativos; tudo isso no ciberespaço.

O tratamento massificado de dados não é uma exclusividade das organizações privadas. É uma realidade também no setor público. Há tempos o Poder Público lida com informações dos seus cidadãos. Devido aos constantes avanços das tecnologias da informação e comunicação, e a transformação dos dados em oportunidades econômicas de novos conhecimentos e serviços, a Administração Pública viu a necessidade de ingressar no ambiente digital.

A Administração Pública é um dos maiores interessados na coleta e tratamento de dados, e constantemente exige de seus cidadãos a exposição de suas informações pessoais, seja para a prestação de serviços públicos, seja para o direcionamento de implementação de políticas públicas. As mais diversas pessoas jurídicas e órgãos que formam a estrutura administrativa acumulam dados pessoais da população. Desde o nascimento, com o registro civil em um cartório, o Poder Público reúne dados dos particulares. Praticamente todos atos da vida acabam sendo informados a uma repartição pública: casamento, filhos, separação, morte, cadastros em órgãos de saúde, de educação, do trabalho, de trânsito, fiscais, previdenciários, eleitorais, imobiliários, financeiros, processuais. Do nascimento à morte, e até após, o Poder Público coleta, trata, armazena, transmite e arquiva dados pessoais dos cidadãos.

Como dizem Luciano Reis e Rafael Lippman

> [...] não é exagerado afirmar que o Estado tem seus olhos postos sobre todos os aspectos da vida de cada um dos cidadãos que o conformam. Nascimento, grau educacional, bens, movimentações financeiras, laborativas, infrações cometidas, enfim, toda a gama de informações relacionadas à vida e a personalidade, várias delas qualificadas como *sensíveis*. (Reis; Lippmann, 2021, p. 170).

Embora o que tenha mais chamado a atenção e impulsionado a criação de leis com a finalidade de proteção dos dados seja o seu tratamento pelas grandes empresas privadas, conhecidas como *Big Techs*, pode-se ver que o Poder Público é o principal controlador de dados dos seus cidadãos. Se comparar qualitativamente com os dados colhidos pelas empresas privadas, há muito mais informações pessoais em posse dos órgãos públicos.

Não sem razão, o uso de dados dos cidadãos para realizar serviços públicos ou implementar políticas públicas no ciberespaço estão sujeitos aos diplomas legais que tratam das relações jurídicas no ambiente digital, sobretudo da Lei n. 13.709, de 14 de agosto de 2018 (LGPD). Se, ao lado dos particulares, a Administração Pública coleta, armazena e utiliza-se de dados pessoais de seus cidadãos, o uso indevido desses dados não é exclusividade do setor privado.

A submissão do Poder Público à LGPD visa trazer segurança jurídica à relação pública com os dados dos particulares, contribuindo para a mitigação do risco de violação dos direitos fundamentais dos titulares dos dados, sem que comprometa a execução do serviço público e das competências legais administrativas. (Zilioto; Greggio, 2021, p. 191).

Ainda, é preciso lembrar que a Administração Pública possui a prerrogativa de compartilhar dados pessoais sem o prévio e expresso consentimento do seu titular. Em outras palavras, ela pode usar os dados pessoais de um cidadão independentemente de seu conhecimento.

Valer-se do ambiente digital em busca de melhorar a eficiência administrativa para atingir o interesse público não significa que o Poder Público se encontra liberto das amarras do direito. Nesse passo, o agir administrativo no ciberespaço é tutelado pelo microssistema do ambiente digital cujas regras precisam ser lidas sob as lentes das particularidades que o regime jurídico administrativo apresenta, sobretudo a sua carga axiológica.

2 Aplicabilidade do microssistema jurídico do ambiente digital à Administração Pública

Como já apontado por Caio Sperandéo de Macedo e outros (2023), há elementos suficientes para a construção de um microssistema jurídico do ambiente digital com o

objetivo de tutelar a proteção de dados e a aplicação das novas tecnologias na sociedade, com fins de preservar os direitos fundamentais e humanos. O microssistema do ambiente digital trata dos conflitos sociais que decorrem da constante inovação das TICs, para que não fiquem alijados de uma efetiva proteção jurídica.

O microssistema do ambiente digital é identificado por (i) uma legislação estruturante, (ii) princípios básicos novos e específicos e (iii) institutos próprios. A aglutinação desses elementos permite não apenas construir o microssistema jurídico do ambiente digital, como também articular a sua aplicação às relações que envolvem a Administração Pública.

2.1 Legislação estruturante

O primeiro passo para a construção de um microssistema, é identificar os textos normativos que versam sobre o tema. É a legislação, em sentido amplo, que dará sustentação à tutela dos indivíduos diante das complexidades trazidas pelas tecnologias. A Constituição Federal, nesse contexto, é a viga mestra da construção de um microssistema do ambiente digital com solidez. Lá constam diversos princípios que servem de alicerce para uma efetiva proteção do ser humano no ambiente digital, esteja ele em uma relação jurídica privada ou em uma relação jurídica pública. A inclusão do inciso LXXIX ao art. 5º da Constituição, assegurando a proteção de dados pessoais, inclusive no meio digital, torna-se núcleo protetivo dos novos conflitos que decorrem da Sociedade da Informação.

Antes mesmo da explícita aparição no rol dos direitos fundamentais, a proteção de dados já vinha conquistando autonomia[89], uma vez que se correlaciona com outros direitos fundamentais tradicionalmente consagrados como a privacidade, a liberdade de expressão, a intimidade, a inviolabilidade, ou seja, compõe a dignidade do ser humano.

Com a consolidação da Sociedade da Informação, a tutela dos dados pessoais adquire importância ainda maior, chamando a atenção dos legisladores a necessidade de

[89] Nesse sentido se expressou Danilo Doneda (2011, p. 103): "No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada".

uma efetiva regulamentação. Passa a integrar, ainda de forma tímida, textos normativos, como o Marco Civil da Internet, até ganhar uma lei específica, a Lei n. 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados.

Nesse passo, o reconhecimento expresso da proteção de dados pessoais como direito fundamental pela Emenda Constitucional n. 115 de 2022 sedimenta o caminho para a formação do microssistema jurídico do ambiente digital ao lado da Lei n. 13.709, de 14 de agosto de 2018 (LGPD).

Embora se reconheça a relevância da LGPD como o ponto de partida para a organização do microssistema jurídico do ambiente digital, ela não é suficiente para dar um efetivo tratamento aos diversos conflitos sociais que emergem no ambiente digital. As crescentes complexidades sociais decorrentes da contínua e exponencial evolução tecnológica mostram que uma única lei não tem a capacidade de solucionar todas as demandas que aparecem. Por isso, a proposta doutrinária de construção do microssistema jurídico do ambiente digital em torno do direito fundamental à proteção de dados não obstrui o diálogo com outros textos normativos.

A estruturação do microssistema jurídico do ambiente digital, portanto, engloba outros diplomas legais. Pode-se, a titulo exemplificado, mencionar a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), a Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e a Lei n. 8.078. de 11 de setembro de 1990 (Código de Defesa do Consumidor). São normas que contribuem significativamente com uma efetiva proteção dos direitos fundamentais em virtude dos conflitos sociais na Sociedade da Informação.

O microssistema jurídico do ambiente digital tutela não só as relações sociais digitais dos particulares. O Poder Público, como já observado, age no ciberespaço. As mais diversas instituições públicas são grandes acumuladoras de dados pessoais. Ao nascer, o cidadão já tem a sua identificação registrada em um órgão público. E segue transmitindo dados para os órgãos públicos por toda sua vida. Reconhecendo esse elevado volume de informações que a Administração Pública possui sobre a sua população, a própria Lei n. 13.709/2018 (LGPD), logo no seu art. 1º, apresenta como um dos seus objetivos o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa jurídica direito

público. Ademais, dedica o Capítulo IV ao tratamento de dados pessoais pelo Poder Público.

A atuação da Administração Pública no ambiente digital não se restringe ao tratamento de dados. Vai além. Há uma série de serviços públicos que são prestados *on line*: requerimento de certidões, processos administrativos, consultas, requisição de benefícios, fornecimento de informações, licitações. Por isso, o tratamento das relações jurídicas que têm a participação do Estado reclama um diálogo com outros textos legais, até mesmo em virtude do princípio da unidade do direito. Ao se tratar da atuação da Administração Pública no ambiente digital é possível apontar outros diplomas legais que englobam a temática: Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação); Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Lei n. 14.063, de 23 de setembro de 2020 (trata do uso de assinaturas eletrônicas em interações com entre públicos) e a Lei n. 14.123, de 29 de março de 2021 (Lei do Governo Digital).

As normas que tratam da atuação do Poder Público no ambiente digital são estruturadas a partir dos princípios constitucionais e seguem pela legislação infraconstitucional em um contínuo diálogo de textos legais, com o objetivo de tratar dos mais variados campos do direito que tutelam as condutas realizadas virtualmente.

2.2 Princípios básicos específicos

Ao lado da legislação que estrutura o microssistema jurídico do ambiente digital, é possível identificar princípios básicos específicos que lhe darão uma sólida sustentação. São diretrizes axiológicas que a tutela jurídica deve preservar ao resolver os conflitos sociais na Sociedade da Informação.

Danilo Doneda (2011, p. 98), após apresentar a evolução das leis sobre proteção de dados pessoais em busca de modelos jurídicos mais completos, verifica que há uma tendência de consolidação de certos princípios básicos já presentes nas primeiras gerações e com vinculação cada vez mais estreita com a proteção da pessoa e com os direitos fundamentais. No início da década de 1980 surgem medidas que são encontradas em textos legais diversos, formando um conjunto de princípios a serem aplicados na proteção de dados.

São princípios que, mesmo desmembrados ou adaptados, integram o núcleo central de leis, tratados, acordos e outros textos legais que versam acerca da proteção de dados. Tais princípios são assim sistematizados: (i) *princípio da publicidade*, ou da transparência, que determina o conhecimento público dos bancos de dados existentes; (ii) *princípio da exatidão*, exigindo a fidelidade dos dados à realidade, implicando em uma coleta com cuidado e correção, com atualizações periódicas; (iii) *princípio da finalidade*, segundo o qual a utilização de dados deve estar de acordo com a finalidade comunicada ao interessado antes da coleta; (iv) *princípio do livre acesso*, que garante o acesso do indivíduo ao banco de dados em que as suas informações estão armazenadas, inclusive com a possibilidade de controle; (v) *princípio da segurança física e lógica*, cuja finalidade é assegurar a proteção dos dados contra extravio, destruição, modificação, transmissão ou acesso não autorizado. (Doneda, p. 100-101).

Ademais, a própria Lei n. 13.709, de 14 de agosto de 2018 (LGPD) traz um expressivo conteúdo principiológico, relacionado com os princípios acima citados. Citando apenas o art. 6º, há uma lista de dez princípios que o tratamento de dados deve observar: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança, (viii) prevenção; (ix) não discriminação; e (x) responsabilização e prestação de contas.

São, ao menos, esses princípios que o processo de positivação de normas dentro do ambiente digital deve sempre se apoiar. Não se deve esquecer que há princípios constitucionais que estão umbilicalmente conectados com a tutela dos dados pessoais. O rol de princípios apresentados na LGPD são simétricos a muitos já previstos no texto constitucional, como aqueles relacionados a inviolabilidade da intimidade, da honra, da imagem e da privacidade das pessoas. Ou seja, não se pode descartar a carga axiológica contida na Constituição Federal de 1988. Afinal, há uma estrutura hierárquica no direito, com as normas constitucionais irradiando efeitos sobre todas as demais que integram o ordenamento jurídico.

Não se pode negar o princípio da unicidade do direito, cujo papel central e proeminente é da Constituição, capaz de unificar a legislação infraconstitucional por manifestar os valores da sociedade. Por isso, os princípios constitucionais são de extrema importância no exercício da aplicação e interpretação do direito, inclusive no microssistema

do ambiente virtual. O microssistema do ambiente digital tem de ser construído sobre os aspectos axiológicos da Constituição Federal de 1988, sobretudo o princípio da dignidade do ser humano. (Macedo; *et. al.*, 2023).

Tais princípios compõem a estrutura fundante para uma proteção jurídica dos dados pessoais sempre relacionada aos direitos fundamentais. A principiologia que organiza o microssistema jurídico do ambiente digital, portanto, se estrutura a partir do texto constitucional com o direito fundamental à proteção de dados e os valores consagrados em prol da dignidade humana, perpassando por princípios comuns que asseguram uma efetiva proteção dos dados pessoais, incluindo aqueles explicitamente previstos na Lei n. 13.709, de 14 de agosto de 2018 (LGPD).

Todavia, esses princípios, quando se trata da Administração Pública, não podem ser investigados descolados dos tradicionais princípios administrativos. As relações jurídicas administrativas digitais implicam uma conexão dos princípios básicos específicos do microssistema jurídico do ambiente digital com a principiologia que forma o regime jurídico administrativo.

2.3 Institutos jurídicos próprios

A estrutura legislativa somada a princípios específicos deve permitir a construção de institutos jurídicos próprios para que um microssistema tenha a sua autonomia didática. Há alguns elementos que somente dentro da arquitetura do microssistema jurídico do ambiente digital são encontrados.

O próprio conceito de privacidade precisa ser atualizado para englobar os acontecimentos sociais no âmbito digital. A definição proposta em 1890 por Samuel Warren e Louis Brandels, como o direito a ser deixado só, há de ser atualizada, tendo em vista a complexidade das relações sociais hodiernas. Há uma fragilização dos limites da vida privada na Sociedade da Informação principalmente pelo vasto volume de dados pessoais que ficam registrados ao navegar pela internet e pela capacidade, cada vez maior, computacional de processar essas informações. Com isso, privacidade deve englobar distintas perspectivas, inclusive as informações pessoais. É a partir da visão moderna de

privacidade que se começa a fortalecer a ideia de proteção de dados como direito fundamental.

A Lei n. 13.709, de 14 de agosto de 2018 (LGPD) cuida do "tratamento de dados" inclusive no meio digital. Define "tratamento" como toda operação realizada com dados pessoais, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X). O sistema legal desenvolvido para a proteção de dados tem como ponto de partida o seu "tratamento", ou seja, qualquer operação que seja realizada com dados pessoais, representando para o seu titular um instrumento de controle sobre a suas informações pessoais e de garantia de direitos.

O consentimento do titular dos dados recebe uma tutela específica na LGPD, apesar de não ser a única hipótese legal para o seu tratamento contida no seu art. 7º. Consiste em um instrumento jurídico que assegura ao titular dos dados o seu efetivo controle, capaz de autorizar ou proibir atos relacionados ao tratamento desses dados pessoais. A pessoa titular dos dados deve autorizar de forma explícita e inequívoca que suas informações sejam usadas por empresas ou órgãos públicos. Deixa claro que o titular dos dados é a pessoa a quem eles dizem respeito e não que o utiliza ou armazena.

O atual cenário da Sociedade da Informação prevê uma comoditização dos dados pessoais proporcionada pela amplitude computacional cada vez mais desenvolvida. A mercantilização dos dados demanda um maior cuidado com o consentimento do titular para o tratamento dessas informações. Por isso, o "consentimento" requer uma investigação própria relacionada ao tratamento de dados no ambiente digital. É como afirma Danilo Doneda (p. 295, 2020):

> A qualificação jurídica do consentimento para o tratamento de dados pessoais não deve ser tomada como uma tarefa que visa ao enquadramento da sua disciplina em um esquema preconcebido, no qual o tratamento de dados pessoais deva submeter-se aos cânones de uma determinada concepção da autonomia privada. A especificidade do consentimento, no caso da proteção dos dados

> pessoais, pede igualmente uma funcionalização de sua própria natureza jurídica, e ao intérprete cabe integrar essa disciplina do consentimento com os efeitos que dela são pretendidos.

Percebe-se, portanto, que existe uma necessidade de se estudar o "consentimento" como uma categoria que pertence ao microssistema jurídico do ambiente digital, separado da sua tradicional natureza puramente negocial integrante do direito civil.

Brevemente, demonstrou-se a existência dos institutos jurídicos da "privacidade", do "tratamento de dados" e do "consentimento" que integram e sustentam o microssistema do ambiente digital. Já no que diz respeito ao direito público, há institutos que lhe são próprios, e que podem ser relacionados com as novas tecnologias da informação, caracterizando de forma contundente o agir administrativo no ambiente digital. Cita-se como exemplo a licitação, que na Sociedade da Informação vem encampando o formato eletrônico. O art. 12 da Lei n. 14.133, de 1º de abril de 2021, estabelece que os atos, no processo licitatório, serão preferencialmente digitais, de forma a permitir que sejam produzidos, comunicados, armazenados e validados por meio eletrônico.

3 O Regime Jurídico Administrativo no ambiente digital

A digitalização das condutas humanas, inclusive aquelas realizadas pelo Estado, implicam um novo paradigma, que rompe com a tradicional ordem social. Esse paradigma conduz a uma interação do Estado com as novas tecnologias da informação e comunicação e expõe a relevância de se lançar olhares mais acurados na investigação e interpretação do Direito Administrativo, sobretudo no que se refere à preservação dos direitos fundamentais na Sociedade da Informação.

O tradicional modelo imperativista do Direito Administrativo é observado na digitalização dos atos administrativos. Os particulares são obrigados a se mudarem para o ambiente digital e lá fornecerem uma série de informações ao Poder Público para que tenham acesso a determinados serviços públicos. Para se tornar cidadão, ter direito a votar e ser votado, não basta um simples cadastro. O Estado brasileiro exige a biometria. Sem providenciar esse dado, não é possível votar, o que pode gerar outros tipos de sanção.

Estruturar o regime jurídico administrativo no princípio da supremacia do interesse público é desequilibrar, a favor do Estado, as suas relações com os particulares. Preestabelecer a sobreposição do interesse público sacrifica o particular, não valorando os direitos fundamentais que consolidam o Estado Democrático de Direito.

A atuação da Administração Pública no ambiente digital precisa ser pautada não só pela estrutura que compõe o microssistema jurídico organizado para tratar dos conflitos gerados em virtude das novas tecnologias da informação, como também pelo regime jurídico administrativo, sobretudo pelos princípios constitucionais que balizam o agir dos entes públicos. Dentre eles, destaca-se o rol explicitamente previsto no *caput* do art. 37 da Constituição Federal de 1988, que orienta os atos administrativos.

Por isso, em um ambiente inovador, composto por relações sociais cada vez mais complexas, é preciso conciliar a busca do Estado pelo interesse público com os direitos fundamentais, individuais e coletivos, dos seus cidadãos. Na Sociedade da Informação, com a digitalização da vida, reconhece-se a necessidade de uma reconstrução do regime jurídico administrativo.

Referências

BREGA, José Fernando Ferreira. Perspectivas sobre a Lei do Governo Digital. *In*: CRAVO, Daniela Copetti; JOBIM, Eduardo; FALEIROS JÚNIOR, José Luiz de Moura. (coords.). Direito público e tecnologia. Indaiatuba: Editora Foco, 2022.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law, v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 3 set. 2023.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MACEDO, Caio Sperandeo de; *et al.* Microssistema jurídico do ambiente digital. São Paulo: Ed. dos Autores, 2023.

REIS, Luciano Elias; LIPPMANN, Rafael Knorr. A Administração Pública na Lei Geral de Proteção de Dados. *In:* PIRONTI, Rodrigo (coord). Lei Geral de Proteção de Dados: estudos

sobre um novo cenário de governança corporativa. 1 reimp. Belo Horizonte: Fórum, 2021. p. 167-178.

ZILIOTTO, Mirela Miró; GREGGIO, Felipe. Fundamentos da Lei Geral de Proteção de Dados pessoais e a responsabilidade extracontratual do Estado no tratamento de dados pessoais. *In*: PIRONTI, Rodrigo. (coord). Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa. Belo Horizonte: Fórum, 2021. p. 179-199.