II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS

T255
Tecnologias disruptivas, direito e proteção de dados [Recurso eletrônico on-line] organização II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Larissa Maia Freitas Salerno Miguel, Alexandre Kehrig Veronese Aguiar e Nelson Remolina Angarita – Franca: Faculdade de Direito de Franca, 2024.

Inclui bibliografia
ISBN: 978-65-5274-018-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Regulação do Ciberespaço.
1. Proteção de Dados. 2. Smart Contracts. 3. Propriedade Intelectual. 4. Políticas Públicas de Desenvolvimento. 5. Efetividade do Direito. I. II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2024 : Franca, SP).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS

Apresentação

Entre os dias 27 e 30 de agosto de 2024, a Faculdade de Direito de Franca recebeu o Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 3 – Tecnologias Disruptivas, Direito e Proteção de Dados concentrou-se na análise das tecnologias disruptivas e seus impactos sobre o direito e a proteção de dados pessoais. As discussões abordaram a regulação jurídica de startups, lawtechs e legaltechs, além da tributação e da propriedade intelectual em um cenário de inovação constante. Entre os temas centrais, destacaram-se as implicações das tecnologias da quarta revolução industrial, como a realidade aumentada, o Visual Law, e os contratos inteligentes (smart contracts), que estão moldando o futuro das relações jurídicas. Foi dado especial enfoque à economia do conhecimento e à crescente coleta e tratamento de dados pessoais e sensíveis, considerando os desafios da proteção de dados, vigilância, monitoramento e remoção de conteúdo. As contribuições deste GT oferecem uma visão crítica e propositiva para o direito acompanhar as rápidas mudanças tecnológicas, promovendo a segurança jurídica e o respeito aos direitos fundamentais na era digital.

O ANTAGONISMO ENTRE A ERA DIGITAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

THE ANTAGONISM BETWEEN DIGITAL ERA AND THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION

Fernanda Nascimento Faleiros [1]
Matheus Lacerda Verzola [2]

Resumo

Os dados pessoais são o ativo principal na atual era da informação digital, sendo inclusive tratados como valiosa mercadoria pelas grandes empresas. Nesse sentido, o presente trabalho visa traçar um panorama sobre o recente reconhecimento do status constitucional da proteção aos dados pessoais, demonstrando como o sistema vem tentando aumentar a segurança jurídica e o poder de proteção judicial sobre tais bens jurídicos, tendo em vista a inegável utilização deturpada das novas tecnologias, que gera danos e prejuízos significativos à sociedade, demonstrando que nem sempre avanço tecnológico e privacidade caminham juntos.

Palavras-chave: Dados pessoais, Novas tecnologias, Segurança jurídica, Proteção judicial

Abstract/Resumen/Résumé

Personal data is the main asset in the current era of digital information, and is even treated as a valuable commodity by large companies. In this sense, the present work aims to provide an overview of the recent recognition of the constitutional status of personal data protection, demonstrating how the system has been trying to increase legal security and the power of judicial protection over such legal assets, taking into account the undeniable use distortion of new technologies, which generates significant damage and losses to society, demonstrating that technological advancement and privacy do not always go together.

Keywords/Palabras-claves/Mots-clés: Personal data, New technologies, Legal security, Judicial protection

[1] Advogada, Pós graduanda em Direito Público pela PUC RS, Graduanda em Psicologia pela Universidade de Franca. Email: fernandafaleiros8@gmail.com

[2] Médico graduado pela Universidade de Franca. Habilitado em Reanimação Neonatal. Email: matheus_verzola@hotmail.com

1. INTRODUÇÃO

A expansão e avanço das novas tecnologias e digitalização da sociedade fez surgir uma crescente preocupação com o tratamento conferido aos dados disponibilizados no meio digital, de modo que a cada dia aumenta a quantidade de legislações relativas ao tema, tendo em vista o valor econômico, político e simbólico que os dados possuem. Nesse sentido, algumas leis e Convenções já preveem tal proteção como direito fundamental, como a Comissão da ONU para Direitos Humanos, jurisprudências da Corte Europeia e do Tribunal de Justiça da União Europeia, a Convenção da União Europeia e a própria Constituição brasileira.

Tendo isso em vista, o presente trabalho busca abordar os fundamentos e princípios da proteção aos dados pessoais, especificando como o ordenamento jurídico brasileiro os trata, algumas classificações, como as de dados sensíveis, sob uma perspectiva de antagonismo em relação aos desafios impostos pela utilização das novas tecnologias de forma exacerbada ou deturpada, que acaba invadindo a esfera do direito à proteção desses dados.

Essa perspectiva garante um objetivo de estudo exploratório e explicativo. Em relação ao método científico empreendido, este será predominantemente dialético, visando uma interpretação dinâmica da realidade, se baseando em uma abordagem qualitativa. Quanto a metodologia de pesquisa, consistirá em estudo bibliográfico sobre a temática referida, baseando-se em análise de doutrinas e artigos de estudiosos da área, publicações jurídicas recentes, bem como em análise documental e de casos controversos

2. FUNDAMENTOS E PRINCÍPIOS DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

O Brasil reconheceu o direito fundamental à proteção de dados recentemente, através da PEC 17/2019, que foi aprovada em fevereiro de 2022, transformando-se na Emenda Constitucional nº115, responsável por alterar a Constituição Federal incluindo a proteção de dados pessoais entre os direitos e garantias fundamentais no art.5º, inciso LXXIX: "É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Apesar de que até então não era um direito fundamental expressamente previsto, a doutrina e jurisprudência tendiam fortemente a reconhecê-lo como tal, especialmente por conta de outras previsões como a do art. 5º, inciso XII, e art. 5º, inciso LXXII, que tratam de temas relacionados à proteção de dados pessoais. Além disso, já vigorava o Código de Defesa do

Consumidor (Lei 8.078/1990), a Lei de Acesso à Informação (Lei 12.527/2011), o Marco Civil da Internet (Lei 12.965/2014) e seu respectivo Decreto regulamentador (Decreto 8.771/2016), com destaque especial para a Lei Geral de Proteção de Dados (Lei 13.709/2018).

Essa tendência mencionada de considerar a proteção aos dados pessoais como direito fundamental antes da EC 115 se dava especialmente porque o Supremo Tribunal Federal realizava uma interpretação conforme alguns princípios e direitos fundamentais, tanto de caráter geral, quanto especial, como o princípio da dignidade da pessoa humana, o direito fundamental ao livre desenvolvimento da personalidade, o direito à liberdade, bem como direitos da personalidade relevantes a temática, isto é, direito à privacidade, à intimidade e à livre disposição sobre os dados pessoais, mais conhecido como direito à livre autodeterminação informativa.

Esse status fundamental foi importante por várias razões, especialmente porque existem lacunas em legislações que tratam sobre o ambiente digital, como é o caso da LGPD, que não contempla os setores da segurança nacional, segurança pública, investigação criminal, execução penal, apenas para citar os mais relevantes. Assim, com o reconhecimento do referido direito fundamental, passa a inexistir uma 'zona livre' de proteção dos dados pessoais na ordem jurídica brasileira (SARLET, 2022, p.11). Ademais, com a inclusão desse direito no rol constitucional, ele assume o caráter de limite material à reforma constitucional, de modo a impedir tentativas de supressão via emenda constitucional.

Ressalta-se que a doutrina e o STF têm reconhecido a dupla dimensão do direito à proteção de dados pessoais, isto é, uma subjetiva e outra objetiva. Aquela diz respeito ao direito e dever do titular de dados pessoais previstos na LGPD poder ser conduzido à proteção constitucional, já que se trata de uma interpretação possível mesmo que não tivesse prevista em lei infraconstitucional. Nesse sentido, decorre o direito de solicitar 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 (SARLET, 2022, p.12).

Quanto a dimensão objetiva, baseia-se no reconhecimento de que esses deveres de proteção vinculam todos os órgãos estatais, além de tornar possível a aplicação no ordenamento jurídico brasileiro, via jurisprudência, da proibição de proteção insuficiente, pregada pelos alemães desde a elaboração da Lei de proteção de dados de Hesse, a primeira lei conhecida de proteção de dados, introduzida em 1970.

3. OS DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA DIGITAL

Atualmente passamos pela chamada "sociedade informacional", conceito de Manuel Castells, relativo ao fluxo contínuo de dados, capaz de condicionar a economia, as relações sociais, a cultura, é caracterizada pelos "três V", isto é, volume excessivo de dados, velocidade desse fluxo e variedade na produção desses dados. Estima-se que a cada minuto, 347 mil novos stories são postados no Instagram, 147 mil fotos são publicadas no Facebook e 41 milhões de mensagens são trocadas no WhatsApp[1].

Isso faz com que seja altamente improvável garantir uma ampla proteção aos dados pessoais, especialmente tendo em vista que as pessoas, por convenção social ligado ao uso exacerbado das redes sociais, deliberadamente depositam milhares de dados pessoais na internet sem ao menos pensar em como estes podem gerar um aglomerado de informações capazes de delinear um perfil pessoal completo, inclusive com dados financeiros, posições políticas, ideológicas, religiosas, orientando a ação de empresas e grupos que lucram com o manejo e venda desse tipo de informação.

Assim ficou mundialmente conhecido o caso da Cambridge Analytica, a empresa de análise de dados foi acusada de atuar em prol da campanha eleitoral de Donald Trump e pelo Brexit na Inglaterra. O esquema baseava-se na compra de dados de mais de 50 milhões de usuários do Facebook, usados para manipular os votos dos eleitores. A empresa, em tese, não cometeu nenhum ato de hacker, mas apenas adquiriu os dados, e com eles direcionava mensagens e postagens para os eleitores pró Hillary e pró Trump.

> A empresa [Cambridge Analytica] também fazia uso da rede social Facebook com a prática de ataques-focais (microtargeting, em inglês) de seus usuários, muitas vezes utilizando-se – de forma intencional – de notícias falsas (Fake News) para manipular tendências políticas de eleitores, resultando em uma ruptura da democracia e gerando, de forma deliberada, uma sociedade polarizada (FORNASIER; BECK, 2020, p. 183).

Mas podemos voltar no tempo para falar do tratamento indevido dos dados pessoais, à exemplo do Caso Oliver Sipple, ocorrido nos EUA em 1984, em que Oliver realizou um pedido por privacidade logo após salvar o presidente Gerald Ford de um atentado, já que a partir de então sua vida pessoal e sexualidade haviam sido expostas por ele ter se tornado uma "pessoa pública". Já na época as autoridades, contudo, negaram o seu pedido, afirmando que ao realizar

[1] Os dados são da edição 2020 do infográfico Data Never Sleeps ("Dados não dormem nunca", em tradução livre) da Domo, empresa especializada em computação na nuvem. Mais informações Disponível em < https://www.techtudo.com.br/noticias/2020/08/o-que-acontece-a-cada-minuto-na-internet-estudo-traz-dados-surpreendentes.ghtml> Acesso em 03 jul.2024.

o ato de heroísmo e se tornar uma figura pública, sua vida pessoal tinha se tornado objeto de interesse público.

Também memorável o Caso Amann versus Suíça, em que Hermann Amann havia vendido, pelo telefone, um depilador elétrico a um indivíduo residente na então União Soviética. A chamada havia sido interceptada pelo governo suíço, e ele considerado suspeito de ter ligações com o governo russo, o que levou a seu monitoramento constante. Tal caso foi julgado em 2000 e traz à tona discussões sobre os limites da vigilância governamental em prol da segurança nacional.

Logo, fica evidente que o problema da proteção de dados pessoais não é algo que surgiu recentemente, mas pode-se afirmar com certeza que foi agravado pelo advento da internet e das novas tecnologias, especialmente com as redes sociais, que geram um acúmulo informacional muito grande. O avanço da inteligência artificial também tem causado controvérsias e gerado efeitos na esfera judicial, como ocorreu com a concessionária ViaQuatro, da linha 4 – Amarela do Metrô de São Paulo, multada pela Justiça em R$100 mil. A decisão[2] dada em maio de 2021 foi referente ao uso de um sistema de reconhecimento facial implantado em 2018 para coletar registros biométricos de passageiros. Com a decisão, a empresa também ficou impedida de voltar a usar a tecnologia.

Existem ainda outros precedentes relevantes quanto ao compartilhamento de dados entre instituições públicas e/ou privadas, como a ADPF 695 (2019), sobre o compartilhamento de dados do DENATRAN com a ABIN; a ADI 6387 (2020), acerca do direito fundamental autônomo; o HC 168052/SP (2020) e a proteção de dados armazenados no Whatsapp; o MS 36.150/DF (2018), relativo a entrega de dados do ENEM ao TCU. Vejamos um trecho do acórdão deste último:

> 1. Mandado de segurança impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira - INEP contra acórdão do TCU que determinou a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família. 2. O art. 5o, X, XIV e XXXIII, da CF/1988, e a Lei no 12.527/2011 asseguram o sigilo de dados pessoais. A divergência quanto ao dever de sigilo do INEP sobre os dados requisitados pelo TCU é matéria sujeita à reserva de jurisdição, não cabendo ao órgão de controle externo decidir sobre a caracterização de ofensa à garantia constitucional. 3. As informações prestadas ao INEP são fornecidas por jovens estudantes para o atendimento de uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo das informações pessoais. É plausível a alegação de que a transmissão desses dados para finalidade diversa: (i) subverte a autorização daqueles que concordaram em prestar as declarações; e (ii) coloca em risco a capacidade do INEP de pesquisar e monitorar políticas públicas.

[2] Processo n. 1090663-42.2018.8.26.0100.

Logo, é notável que o Brasil tem se empenhado em avançar na proteção dos dados pessoais, inclusive com a criação da Autoridade Nacional de Proteção de Dados (ANPD), um órgão vinculado à Presidência da República, dotado de autonomia técnica e decisória, que tem a competência de zelar pela proteção dos dados pessoais, visando proteger os direitos fundamentais de liberdade e privacidade, garantindo o livre desenvolvimento da personalidade da pessoa natural. Todavia, isso não é uma tarefa fácil quando o contexto mundial tecnológico que a sociedade experimenta é desfavorável, especialmente quando considerado o aumento dos *data leaks* (vazamento de dados), inclusive de dados sensíveis.

Os dados sensíveis são conceituados pela LGPD em seu artigo 5º, inciso II, como os que versam 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.

Vale mencionar a decisão super recente da ANPD, que emitiu no dia 02 de julho de 2024 uma Medida Preventiva determinando a imediata suspensão, no país, da vigência da nova política de privacidade da empresa Meta (Facebook, Messenger e Instagram), que autorizava o uso de dados pessoais publicados em suas plataformas para fins de treinamento de sistemas de inteligência artificial (IA).

A ANPD realizou a instauração de ofício dessa fiscalização, diante dos indícios de violações à LGPD, sendo que, conforme o Voto nº 11/2024/DIR-MW/CD, aprovado pelo Conselho Diretor em Circuito Deliberativo, a Medida Preventiva se justificava diante de algumas circunstâncias autorizadoras: uso de hipótese legal inadequada para o tratamento de dados pessoais; falta de divulgação de informações claras, precisas e facilmente acessíveis sobre a alteração da política de privacidade e sobre o tratamento realizado; limitações excessivas ao exercício dos direitos dos titulares; e tratamento de dados pessoais de crianças e adolescentes sem as devidas salvaguardas.

Ademais, a autarquia não considerou válida, ao menos preliminarmente, a justificativa dada pela empresa para o tratamento dos dados pessoais, isto é, o "legítimo interesse da empresa". Até porque tal hipótese não é aplicável em casos que envolvam o tratamento de dados pessoais sensíveis, além de não condizer com os princípios da finalidade e da necessidade. Por fim, foi ponderado que seriam utilizados para treinar os sistemas de IA da Meta os dados pessoais de crianças e adolescentes, incluindo fotos, vídeos e postagens, também poderiam ser coletados e utilizados para treinar os sistemas de IA da Meta, o que não guarda relação direta

com o melhor interesse dos mesmos, e muito menos observava a adoção de salvaguardas e medidas de mitigação de risco.

4. CONSIDERAÇÕES FINAIS

De acordo com as novas legislações sobre proteção de dados, especialmente a LGPD, e com o reconhecimento da proteção aos dados pessoais como direito fundamental a partir da EC 115/22, fica evidente que o Brasil tem dado grandes passos em direção a garantia de mais segurança no meio digital, buscando demonstrar que ao contrário do que popularmente se prega, não se trata de uma "terra sem lei". Todavia, o país, e quiçá grande parte do mundo, ainda está bem longe de conseguir garantir uma verdadeira segurança jurídica ao tratamento dos dados pessoais.

O levantamento divulgado pela empresa de soluções de cibersegurança Fortinet, utilizando dados do FortiGuard Labs, indicou que o Brasil foi o segundo país mais atingido da América Latina em 2022 quanto a ataques cibernéticos, com 103,16 bilhões de tentativas de ataques[3]. Isso demonstra que ainda há extremas e extensas fragilidades no sistema de proteção cibernético brasileiro, que demandará esforços conjuntos para ao menos atenuar tal situação. Nesse sentido, é preciso que se desenvolva uma conscientização sobre a importância da segurança cibernética, posto que a maioria das pessoas e das empresas sequer tem o mínimo de conhecimento para conseguir proteger seus dados e sistemas de forma eficiente, sendo necessário inclusive investir nesse aprendizado.

Além disso, muitas empresas brasileiras se valem de uma infraestrutura tecnológica ultrapassada, que não acompanhou os avanços, deixando-as vulneráveis aos ataques cibernéticos, inclusive a fraudes bancárias. E a esse tópico em especial acrescenta-se que o Brasil passa por um período em que há um significativo aumento de cibercrimes, desde ataques de phishing, ransomware, fraudes online, até crimes mais graves como invasão de dispositivos eletrônicos com finalidade de extorsão, pornografia de vingança, e outros, em que os dados, especialmente sensíveis, ficam totalmente desprotegidos.

[3] FebrabanTech. Brasil é segundo país mais atingido por ciberataques na América Latina, diz relatório. Disponível em <https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio> Acesso em 03 jul. 2024.

Assim, esse Big Data, em tradução livre, “dados gigantescos”, relativo ao conjunto dessa ampla variedade de dados, que exige ferramentas especiais para comportá-los, tratá-los, organizá-los, transformando-os em informação, demanda uma prestação positiva do Estado, como estamos vendo ocorrer. Mas isso também pode ser uma via de mão dupla, e conduzir aos perigos de que o deslumbre com as tecnologias gere um Estado totalitário que interfira no meio digital até quando isso não seja essencial, gerando a necessidade da chamada “Separação Informacional de Poderes” (Miriam Wimmer, 2020).

REFERÊNCIAS

BRASIL, **Lei 12.965** de 23 de abril de 2014. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 02 jul. 2024.

BRASIL, **Lei 13.709** de 14 de agosto de 2018. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 02 jul. 2024.

BRASIL. Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental (ADPF) 695**. Relator(a): Min. Gilmar Mendes, Julgamento: 15/09/2022. Publicação: 19/06/2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta De Inconstitucionalidade 6.387**. Relatora: Min. Rosa Weber.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

FORNASIER, Mateus de Oliveira; BECK, Cesar. **Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia**. Revista Direito em Debate, Ijuí, v. 272 | Revista da Defensoria Pública RS | Porto Alegre, ano 14, v. 2, n. 33, p. 253-274, 2023.29, n. 53, jan./jun. 2020. Disponível em: https://doi.org/10.21527/2176-6622.2020.53.182-195. Acesso em: 03 jul. 2024.

Ministério da Justiça e Segurança Pública. Site Gov. **ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta> Acesso em 03 jul. 2024.

RODRIGUEZ, Daniel Piñeiro. **O Direito Fundamental à proteção de dados: vigilância, privacidade e regulação**. Rio de Janeiro, Lumen Juris, 2021.

SARLET, Ingo W.; SARLET, Gabrielle B S.; BITTAR, Eduardo C B. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital** . São Paulo, SRV Editora LTDA, 2022. E-book. Acesso em: 02 jul. 2024.