XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

JOSÉ RENATO GAZIERO CELLA

JÚLIA FRANCIELI NEVES DE OLIVEIRA

SALETE ORO BOFF

Copyright © 2018 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sudeste - Prof. Dr. César Augusto de Castro Fiuza - UFMG/PUCMG – Minas Gerais
Vice-presidente Nordeste - Prof. Dr. Lucas Gonçalves da Silva - UFS – Sergipe
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Secretário Executivo - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - Unimar/Uninove – São Paulo

Representante Discente – FEPODI
Yuri Nathan da Costa Lannes - Mackenzie – São Paulo

Conselho Fiscal:
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. Aires José Rover - UFSC – Santa Catarina
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP – São Paulo
Prof. Dr. Marcus Firmino Santiago da Silva - UDF – Distrito Federal (suplente)
Prof. Dr. Ilton Garcia da Costa - UENP – São Paulo (suplente)

Secretarias:
Relações Institucionais
Prof. Dr. Horácio Wanderlei Rodrigues - IMED – Rio Grande do Sul
Prof. Dr. Valter Moura do Carmo - UNIMAR – Ceará
Prof. Dr. José Barroso Filho - UPIS/ENAJUM– Distrito Federal
Relações Internacionais para o Continente Americano
Prof. Dr. Fernando Antônio de Carvalho Dantas - UFG – Goías
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Maria Aurea Baroni Cecato - Unipê/UFPB – Paraíba

Eventos:
Prof. Dr. Jerônimo Siqueira Tybusch UFSM – Rio Grande do Sul
Prof. Dr. José Filomeno de Moraes Filho Unifor – Ceará
Prof. Dr. Antônio Carlos Diniz Murta Fumec – Minas Gerais

Comunicação:
Prof. Dr. Matheus Felipe de Castro UNOESC – Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Prof. Dr. Caio Augusto Souza Lara - ESDHC – Minas Gerais

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP – Pernambuco

E27

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS

Coordenadores: José Renato Gaziero Cella; Salete Oro Boff; Júlia Francieli Neves de Oliveira. – Florianópolis: CONPEDI, 2018.

Inclui bibliografia
ISBN: 978-85-5505-726-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Tecnologia, Comunicação e Inovação no Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVII Encontro Nacional do CONPEDI (27 : 2018 : Porto Alegre, Brasil).

CDU: 34

Conselho Nacional de Pesquisa e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

Universidade do Vale do Rio dos Sinos
Porto Alegre – Rio Grande do Sul - Brasil
http://unisinos.br/novocampuspoa/

XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

No XXVII Congresso Nacional do CONPEDI, realizado de 14 a 16 de novembro de 2018, que teve lugar na Universidade do Vale do Rio dos Sinos - UNISINOS, em Porto Alegre-RS, o grupo de trabalho "Direito, Governança e Novas Tecnologias II" se destacou no evento não apenas pela qualidade dos trabalhos apresentados, mas pelo numeroso público, composto por pesquisadores-expositores e interessados, que deixou a sala repleta até o término das atividades. Foram apresentados 19 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente.

Esse fato demonstra a inquietude que o tema desperta na seara jurídica. Cientes desse fato, os programas de pós-graduação em Direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao Direito. Pode-se agrupar os trabalhos apresentados em quatro grandes temáticas, que se congregam nesta coletânea.

Houve enfoque nas possibilidades e contingências democráticas das novas tecnologias, tanto no âmbito teórico quanto no âmbito prático, com apresentações e debates dos seguintes artigos:,

1. POLÍTICAS PÚBLICAS E NEUTRALIDADE DA REDE NO BRASIL;

2. OS DEPARTAMENTOS JURÍDICOS E AS EMPRESAS MULTINACIONAIS DE TECNOLOGIA DA INFORMAÇÃO (TI) QUE ATUAM EM PAÍSES EMERGENTES: A GERAÇÃO DE VANTAGENS COMPETITIVAS À LUZ DAS CAPACIDADES DINÂMICAS;

3. PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO: UMA VISÃO SOB O ASPECTO DOS DIREITOS DA PERSONALIDADE NO BRASIL E NA UNIÃO EUROPEIA;

4. "CORPO ELETTRONICO" COMO VÍTIMA EM MATÉRIA DE TRATAMENTO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL POR DANOS À LUZ DA LEI DE PROTEÇÃO DE DADOS BRASILEIRA E DANO ESTÉTICO NO MUNDO DIGITAL;

5. O VOTO DISSIDENTE DE SOCIO MINORITARIO COMO FORMA DE GESTAO DO RISCO NANOTECNOLOGICO;

6. DEMOCRACIA E TECNOLOGIA: A ELABORAÇÃO DE NOVOS INSTRUMENTOS PARTICIPATIVOS NOS MUNICÍPIOS;

7. PARTICIPAÇÃO DA SOCIEDADE CIVIL NO CONTEXTO DA UNIÃO EUROPEIA: UM ESTUDO DE CASO DA FERRAMENTA EU-PILOT;

8. DIREITO E MEDICINA: UMA VISÃO INTERDISCIPLINAR FRENTE AOS APLICATIVOS PARA MARCAÇÃO DE CONSULTAS MÉDICAS E O POSICIONAMENTO DOS CONSELHOS PROFISSIONAIS;

9. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: NATUREZA JURÍDICA E A LEI Nº 13.079/2018;

10. GESTÃO DOS ASPECTOS JURÍDICOS DA INOVAÇÃO DISRUPTIVA;

11. REFLEXÕES SOBRE A AUTOMAÇÃO NO DIREITO: LAW TECHS;

12. POLÍTICA REGULATÓRIA PARA TECNOLOGIAS DISRUPTIVAS NO BRASIL: O CASO DA TECNOLOGIA BLOCKCHAIN E TECNOLOGIAS DE REGISTRO DISTRIBUÍDAS;

13. O PRINCÍPIO DA PUBLICIDADE E DA FUNDAMENTAÇÃO DAS DECISÕES JUDICIAIS FRENTE A UTILIZAÇÃO DE ALGORITMOS NO DESEMPENHO DA ATIVIDADE JURISDICIONAL E DOS ATOS PROCESSUAIS;

14. ACCOUNTABILITY DE FAKE NEWS: BUSCANDO A VERDADE DA NOTÍCIA FALSA;

15. DIGITALIZAÇÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO – VIRTUALIZAÇÃO E DESMATERIALIZAÇÃO. SATISFAÇÃO DO INTERESSE PÚBLICO – GOVERNO ELETRÔNICO;

16. O DIREITO HUMANO À INTIMIDADE NA CONTEMPORANEIDADE E SEUS DESAFIOS NA SOCIEDADE GLOBALIZADA EM REDE;

17. EFETIVIDADE DO DIREITO À INFORMAÇÃO: DIAGNÓSTICO DA POLÍTICA ESTADUAL DE DADOS ABERTOS GOVERNAMENTAIS NO RIO GRANDE DO SUL;

18. A INCORPORAÇÃO DE DRONES PARA VIGILÂNCIA DE ESPAÇOS URBANOS BRASILEIROS: O USO PELAS FORÇAS ARMADAS E ÓRGÃOS DE SEGURANÇA PÚBLICA DA UNIÃO E DO ESTADO DE SANTA CATARINA; e

19. AUTOCOMUNICAÇÃO E CONTRAPODER: A ARQUITETURA DAS TIC COMO INSTRUMENTOS DE DIFUSÃO INFORMATIVA E O IMPACTO NA AGENDA POLÍTICA

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "direito, governança e novas tecnologias", que trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em Direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores:

Prof. Dr. José Renato Gaziero Cella – IMED

Prof. Dr. Felipe Chiarello de Souza Pinto – UPM

Profa. Dra. Salete Oro Boff - IMED / IESA / UFFS

Nota Técnica: Os artigos que não constam nestes Anais foram selecionados para publicação na Plataforma Index Law Journals, conforme previsto no artigo 8.1 do edital do evento. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

“CORPO ELETTRONICO” COMO VÍTIMA EM MATÉRIA DE TRATAMENTO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL POR DANOS À LUZ DA LEI DE PROTEÇÃO DE DADOS BRASILEIRA E DANO ESTÉTICO NO MUNDO DIGITAL

“ELECTRONIC BODY” AS VICTIM ON THE TREATMENT OF PERSONAL DATA: CIVIL LIABILITY UNDER THE DATA PROTECTION LAW IN BRAZIL AND THE FEASIBILITY OF APPLYING AESTHETIC DAMAGE TO THE DIGITAL WORLD

Cristiano Colombo
Eugênio Facchini Neto

Resumo

O estudo dedica-se ao “corpo elettronico” como vítima de ofensas em matéria de tratamento de dados das pessoas naturais, refletindo sobre a responsabilidade civil por danos e a aplicação da noção de dano estético ao mundo digital. Procura-se demonstrar que no mundo digital o ser humano é vulnerável a danos e que da mesma forma que o corpo humano pode sofrer lesões estéticas que são compensáveis pela via da responsabilidade civil, igualmente o seu “corpo elettronico” pode sofrer danos estéticos no mundo virtual. No que toca à metodologia, a pesquisa foi teórica, exploratória e descritiva, valendo-se de procedimentos técnicos bibliográficos.

Palavras-chave: Corpo eletrônico, Mundo digital, Lei geral de proteção de dados, Responsabilidade civil, Dano estético digital

Abstract/Resumen/Résumé

The study analyzes the "electronic body" as victim of offenses related to the processing of data of natural persons, reflecting on the civil liability for damages and the feasibility of applying aesthetic damage to the digital world. The aim is to demonstrate that in the digital world the human being is vulnerable to damages and that, in the same way that the human body can suffer aesthetic lesions that are compensable, also its "electronic body" can suffer aesthetic damages. Regarding methodology, the research was theoretical, dealing with exploratory and descriptive, using technical bibliographic procedures.

Keywords/Palabras-claves/Mots-clés: Electronic body, Digital world, General data protection law, Civil liability, Digital aesthetic damage

1 INTRODUÇÃO

O estudo tem como propósito dedicar-se ao "corpo elettronico" (RODOTÀ, 2005, p. 120-121) como vítima de ofensas, em matéria de tratamento de dados das pessoas naturais, à luz do texto da nova Lei Geral de Proteção de Dados brasileira (Lei nº 13.709 de 2018), refletindo sobre a responsabilidade civil por danos e a viabilidade da aplicação da noção de dano estético ao mundo digital.

O primeiro capítulo apresentará a noção de "corpo elettronico", discorrendo também sobre o fenômeno da criação de perfis digitais, bem como a identificação de ofensas que lhe atingem, a partir da análise legislativa, jurisprudencial e doutrinária.

O segundo capítulo versará sobre a perspectiva de uma responsabilidade civil por danos à luz da Lei Geral de Proteção de Dados brasileira e a viabilidade da aplicação da noção de dano estético no mundo digital.

A temática é analisada a partir da recente Lei sob o nº 13.709 de 2018, comparando alguns aspectos com o modelo europeu, especialmente após sua recente atualização, através do Regulamento Geral de Proteção de Dados, de 2016.

No que toca à metodologia, a pesquisa foi teórica, tratando do tema em forma exploratória e descritiva, valendo-se de procedimentos técnicos bibliográficos.

2 "CORPO ELETTRONICO" COMO VÍTIMA DE OFENSAS EM MATÉRIA DE TRATAMENTO DE DADOS PESSOAIS

2.1 DO *CORPO ELETTRONICO*

A expressão *corpo elettronico*, assinada por Stefano Rodotà, indica um novo aspecto da pessoa natural, atribuindo-lhe, além da massa física, uma dimensão digital (RODOTÀ, 2005, p. 120-121). O "espaço do corpo" transborda a "unidade física", ultrapassando o "limite delineado pela pele" (RODOTÀ, 2012, p. 26). Uma corpulência "binária" (PEREIRA, 2001, p. 18)[1] se manifesta no mundo virtual com novas partículas que exteriorizam a personalidade, quais sejam: os dados pessoais. Informações reveladas no ciberespaço colaboram para a compleição do corpo eletrônico, comparáveis às "tatuagens, piercing e outros sinais de

[1] Nas palavras do autor: "Fala-se, pois, em ciberespaço, que é o produto da convergência tecnológica da informática, das telecomunicações e do audiovisual. Convergência essa que, por seu turno, é possibilitada pela linguagem binária da informática."

identidade" (RODOTÀ, 2012, p. 322).

Tal fenômeno se acentua na medida em que ferramentas mais precisas de tratamento destes fatos revelados no espaço virtual são desenvolvidas, desde a coleta, classificação, arquivamento, avaliação, sistematização. Tais procedimentos permitem a oferta de *outputs* mais precisos, em face dos dados estarem cada vez mais estruturados. Consequentemente, se a silhueta da pessoa até então era um vulto, passa a ter maior nitidez, riqueza de detalhes, passando de uma sombra para uma intensidade luminar que permite identificá-la claramente. Como coloca NISSENBAUM (2010, p. 36), em capítulo expressivamente intitulado "Knowing Us Better than We Know Ourselves: Massive and Deep Databases", "qualquer coisa sobre um indivíduo pode ser convertido em forma digital, ser armazenado indefinidamente e ser facilmente acessado"

É o que Danilo Doneda (2006, p. 2) refere como "representação virtual", o "avatar" de cada pessoa natural:

> Nossos dados, estruturados de forma a significarem para determinado sujeito uma nossa representação virtual – ou um avatar –, podem ser examinados no julgamento de uma concessão de uma linha de crédito, de um plano de saúde, a obtenção de um emprego, a passagem livre pela alfândega de um país, além de tantas outras hipóteses.

Santaella (2011, p. 39), por sua vez, acentua o entrelaçamento entre o físico e o virtual ao referir sobre a "construção do corpo como parte de um circuito integrado de informação e matéria que inclui componentes humanos e não-humanos, tanto chips de silício quanto tecidos orgânicos, bits de informações e bits de carne e osso". De tal forma, o corpo ligado a uma personalidade deve ser compreendido como o resultante da integração de sua massa física com os dados presentes no ambiente virtual. Ora, mas se os dados representam o elemento constitutivo do corpo eletrônico, como defini-lo?

Segundo Silva, Peres e Boscariolli (2016, p. 384-386), há que se distinguir entre o dado, a informação e o conhecimento. O dado nada mais é um fato, um valor documentado ou um resultado de medição. Atribuindo-se um significado aos dados, gera-se uma informação. E quando estas informações se tornam familiares, permitindo sua apreensão cognitiva, o agente capacita-se a tomar decisões a partir deles – eis aí o conhecimento.

O dado pode ser, por exemplo, o fato que João está acometido de uma doença grave, o que é revelado pelo acesso a um prontuário médico ou a notas fiscais de uma farmácia, que indicam a aquisição de remédios para uma dada patologia. A informação, por sua vez, é interpretar este dado, no sentido de que talvez João venha a faltar alguns dias ao trabalho, em

razão de eventual tratamento, mesmo que isso não necessariamente ocorra. E, o conhecimento seria representado pela não contratação de João para o quadro da empresa, discriminando-o. Danilo Doneda sintetiza esse fenômeno ao referir que "o dado estaria associado a uma pré-informação anterior à interpretação e à elaboração.", enquanto a informação é "algo além da representação contida no dado" (DONEDA, 2006, p. 152).

Dada a importância dos "dados pessoais", sua conceituação passou a integrar os principais elencos legislativos, em nível mundial, como se demonstra através da redação do artigo 4º, 1, do Regulamento Geral sobre Proteção de Dados da União Europeia (2016/679):

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular; (UNIÃO EUROPÉIA, 2016).

Da leitura do texto, depreende-se, no referido instrumento legislativo, um conceito aberto de "dados pessoais", que não se subsume a uma lista taxativa. Consideram-se como tais aqueles que permitam a identificação, mesmo que "em potência". É o que ensina o Manual da Legislação Europeia de Proteção de Dados, ao registrar não haver necessidade de identificação do sujeito para que o dado seja pessoal, ressaltando que, caso seja possível descobrir a pessoa a quem o mesmo se liga, efetuando pesquisas adicionais, enquadra-se neste entendimento. Portanto, o que importa não é a identificação, mas a identificabilidade:

> [C]onsidera-se que as informações contêm dados sobre uma pessoa se: • essa pessoa estiver identificada nessas informações; ou • essa pessoa, embora não esteja identificada, estiver descrita nestas informações de forma que permita descobrir quem é a pessoa em causa efetuando pesquisas adicionais. Ambos os tipos de informações são protegidos da mesma forma na legislação europeia sobre proteção de dados. (MANUAL, 2014, p. 40).

Em Parecer emitido pelo "Grupo de Trabalho de Protecção de Dados do Artigo 29º", que segue sendo aplicado pela União Europeia, mesmo com o advento do Regulamento 2016/679, está registrada o propósito de construir uma "noção ampla", sendo "desejo do Parlamento de que a definição de 'dados pessoais' seja o mais geral possível para incluir toda a informação respeitante a uma pessoa identificável" (PARECER, 2007). Saliente-se, ainda, que "dados pessoais" não são sinônimos a "dados privados" ou "dados sensíveis". Estes se referem às informações que o ser humano revela para si, ou, máximo, aos seus familiares e

amigos próximos, enquadrando-se na antiga noção de privacidade. Já aqueles podem envolver dados profissionais, sociais, incluindo-se aqueles revelados publicamente nas redes sociais[2]. É o que esclarece solarmente dito Parecer:

> A expressão "dados pessoais" inclui informação que toca a esfera da vida privada e familiar da pessoa stricto sensu, mas inclui também informação sobre qualquer tipo de actividade realizada pela pessoa, tal como a que diz respeito às relações de trabalho ou ao seu comportamento económico e social. Inclui, assim, informação sobre pessoas singulares, independentemente do seu estatuto ou papel (consumidor, paciente, empregado, cliente, etc.) (PARECER..., 2007).

Para melhor compreensão da noção de "corpo elettronico", é importante referir o disposto no artigo 4º, 4 do Regulamento Geral de Proteção de Dados da União Europeia, que positiva o "profiling" ou perfil digital. Este é o resultado (*output)* de um algoritmo que subsidia decisões automatizadas por parte dos grandes *players* do mercado. A definição de perfil digital envolve

> qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações; (UNIÃO EUROPÉIA, 2016).

O *profiling* tem como escopo "reunir e analisar dados dos titulares de forma a desenhar perfis comportamentais de consumo, tornando os titulares de dados alvos para o tratamento de dados extremamente intrusivos, como marketing direto" (FAZENDEIRO, 2017, p. 50). Os dados pessoais constituem, portanto, o corpo eletrônico, configurando uma extensão do corpo físico. É o que leciona Doneda (2006, p. 173):

> Esta técnica, conhecida como *profiling*, pode ser aplicada a indivíduos bem como estendida a grupos. Nela, os dados pessoais são tratados, com o auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma "metainformação", que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destinos de uma pessoa ou grupo.

Destaque-se que a Lei Geral de Proteção de Dados brasileira, sob o nº 13.709 de 2018, em seu artigo 5º, II, segue harmoniosamente a legislação europeia, ao definir que:

[2] Interessante notar que desde 1993 (STC 254/1993) o Tribunal Constitucional espanhol reconhece a proteção dos dados pessoais como direito específico e distinto do direito à intimidade, vindo mantendo essa posição na jurisprudência posterior (STC 290/2000 E 292/2000) (ORTIZ, 2005, p. 43)

“dado pessoal: informação relacionada a pessoa natural identificada ou identificável”. Como se vê, ao utilizar a expressão “identificável”, o legislador pátrio reconheceu que, se for possível descobrir de quem se trata, através de “pesquisas complementares”, como referido no Regulamento europeu, também este fato deva ser considerado “dado pessoal”.

Outrossim, a Lei Geral de Proteção de Dados Brasileira, em duas oportunidades, utiliza o conceito de perfil comportamental: a) Artigo 12, § 2º: “Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.”; b) Art. 20: “O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.”.

Por outro lado, no artigo 12 há expressa referência ao termo “perfil comportamental”. Tal expressão colhe o procedimento pelo qual, através da “mineração” dos dados fornecidos pelos próprios usuários ao mundo digital, bem como dos gostos manifestados no ciberespaço, faz-se possível realizar a análise preditiva, no sentido de projetar o foco de interesse ajustado a cada internauta.

O artigo 20, por sua vez, disciplina a possibilidade de se encaminhar pedido de explicação ao controlador dos dados. Nas hipóteses de tratamento de dados unicamente automatizado, o usuário pode exigir uma reanálise por um ser humano. Inegável, portanto, a presença de um corpo eletrônico, decorrente deste fluxo de dados que formam uma massa binária, de zeros e uns (PEREIRA, 2001, p. 18), no mundo digital.

Esse “admirável mundo novo” em que vivemos traz benefícios e vantagens a todos, sem sombra de dúvidas. Todavia, essa nova tecnologia tem potencial para impactar também negativamente nossas vidas. O que afeta nossos avatares virtuais pode vir a afetar sensivelmente nossas existências reais. E, pelas características da rede, o dano pode ser potencializado. Nas palavras de Paesani (2012, p. 77), “parecem evidentes a extensão e o potencial difamatório de uma mensagem divulgada pela rede”. Como se sabe, a técnica e a ciência não aceitam limites. Sua lógica é simples: se pode ser feito, será feito. Cabe ao Direito, municiado pela ética e pelos valores de uma sociedade que formalmente colocou a pessoa humana e sua dignidade como centro de todas as preocupações jurídicas, estabelecer quais os limites e fronteiras que não devem ser ultrapassados ou, se ultrapassados, prever os

remédios cabíveis para compensar eventuais danos ou minorar sua extensão[3]. Como diz Solove (2009, p. 97), "há quem sustente, persuasivamente, que proteger a intimidade é algo impensável na era da informação. Pelo contrário, o Direito pode fazer muito para salvaguardar a intimidade".

2.2 VÍTIMA DE OFENSAS EM MATÉRIA DE TRATAMENTO DE DADOS PESSOAIS

Partindo da existência de dados que identificam uma determinada pessoa ou que possam vir a identificá-la, passando pela formação de perfis comportamentais, chegamos à noção de corpo eletrônico. Diante do direito fundamental à proteção de dados pessoais, mister tutelar os casos de ofensas a esse corpo eletrônico para além do direito à privacidade, pois "as garantias que a princípio eram relacionadas com a privacidade passam a ser vistas através de ótica mais abrangente, pela qual outros interesses devem ser considerados, compreendendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais" (DONEDA: 2006, p. 204-205).

Em estudo mais recente, Doneda (2018) insiste que a proteção de dados tem um enfoque puramente objetivo, não envolvendo os aspectos subjetivos da privacidade[4]. Giusella Finocchiaro (2012, p. 1), de igual forma, salienta as diferenças havidas entre o direito à proteção de dados e as tutelas específicas de direitos já consagrados, como os direitos à privacidade, à integridade, à reputação, à imagem, ao nome. Segundo a autora, o direito à proteção de dados pessoais se referem ao direito do sujeito exercitar um controle ativo sobre seus próprios dados, envolvendo o direito ao acesso e à sua retificação.

Mendes (2014, p. 56) ressalta que é a pessoa humana, em última análise, a

---

[3] Como um efeito colateral do mundo virtual, pela primeira vez na história humana, acessar a informação é mais fácil e mais barato do que esquecer (MAYER-SCHÖNBERGER, 2009, p. 198). Ao longo da evolução da sociedade, a relação entre lembrar e esquecer permaneceu clara: lembrar era caro e difícil, ao passo que esquecer era natural e fácil. Na era digital, em que as informações estão ao alcance dos dedos da mão, em qualquer lugar em que nos encontremos, nada fica no passado e nada é esquecido – todas as informações permanecem disponíveis e acessíveis e o tempo se transformou em um presente contínuo. Os danos causados no mundo virtual, portanto, tem um potencial de duração maior do que no passado. E como alerta Gaudenzi (2017, p. 70), uma potencialidade de dano mais eficaz, já que as redes telemáticas permitem a transmissão das informações a distância e em tempo real.

[4] Discorrendo sobre a privacidade na era da informação, Waldman (2018, p. 150) refere que, por vezes, tentar proteger a privacidade neste mundo dá a sensação de lutar contra moinhos de vento, mas mesmo assim vislumbra possibilidade de êxito, pois estamos cada vez mais cientes dos perigos do acúmulo de dados e tomando medidas para controlar o fenômeno. Já Andreas Weigend, ex-cientista principal da Amazon e fundador do Social Data Lab referiu que o conceito de privacy não mais nos protege na era do *social data*. Segundo ele, "nós não deveríamos estar lutando pela privacy simplesmente porque ela era uma boa resposta para os problemas das pessoas há cem anos atrás" (citado por IGO, 2018, p. 363-364).

destinatária da proteção de dados pessoais, demonstrando a necessidade de elevá-la a um patamar de direito fundamental, já que "constituem um atributo de sua personalidade".

Para verificar como vem se dando essa proteção ao corpo eletrônico, prevenindo-se ofensas ou reparando-se-as, impõe-se a análise de documentos legislativos e judiciais emanados no âmbito da União Europeia, que há tempos vem se dedicando com seriedade à questão, representando uma válida e consagrada experiência, podendo ser tomada como modelo.

a) Parecer 2008/C 110/01

Iniciamos pela análise do parecer exarado pela Autoridade Europeia de Proteção de Dados (AEPD), relativamente à transferência dos dados dos Registros de Identificação dos Passageiros (Passenger Name Record — PNR) com destino ou partida de voos dos Estados-Membros da União Europeia para os Estados Unidos e o Canadá, sob o argumento de "prevenção e luta contra as infracções terroristas e a criminalidade organizada" (PARECER..., 2008). A finalidade apontada foi "identificar pessoas implicadas *ou susceptíveis de estarem* implicadas numa infracção terrorista ou de criminalidade organizada, *bem como os seus associados*." Ocorre que a AEPD reconheceu as seguintes violações ao tratamento de dados, no caso concreto:

a.1) Questões acerca do padrão utilizado (dados utilizados no algoritmo e a construção do perfil). Conforme o trecho do parecer, tem-se que:

> A proposta não dá nenhuma indicação quanto à forma como serão definidos os padrões e efectuada a avaliação de riscos. A avaliação de impacto especifica do seguinte modo a utilização que será feita dos dados PNR: comparar os dados dos passageiros «com uma combinação de características e padrões comportamentais, com o objectivo de realizar uma avaliação de risco. Quando um passageiro corresponde a uma determinada categoria de risco, pode ser identificado como um passageiro de alto risco» (11). [...] As pessoas suspeitas podem ser seleccionadas segundo elementos concretos de suspeição incluídos nos seus dados PNR (p.ex. contacto com uma agência de viagens suspeita, referência de um cartão de crédito roubado) ou com base em «padrões» ou um perfil abstracto. Podem até ser constituídos diferentes perfis normalizados com base nos padrões de viagem, para «passageiros normais» ou «passageiros suspeitos». Tais perfis permitiriam aprofundar a investigação dos passageiros que não entram na «categoria de passageiro normal», por maioria de razão se o seu perfil estivar associado a outros elementos suspeitos, tais como um cartão de crédito roubado [...] (PARECER..., 2008).

De tal forma, como se vê, a primeira violação ao corpo eletrônico se deu pela falta de

transparência do algoritmo aplicado, na construção do *profiling*, bem como a existência de considerável margem de erro, que, a partir de um "método informatizado que utiliza a prospecção de dados num armazém de dados", pode levar uma pessoa inocente vir a ser confundida com um terrorista (PARECER..., 2008).

a.2) Dados Sensíveis

Preocupou-se também referido parecer quanto às ofensas ao corpo eletrônico, na medida em que dados sensíveis, como é o caso de religião, também acabavam por ser transferidos, pois "embora não se possa presumir que os passageiros serão visados conforme a sua religião ou outros dados sensíveis, afigura-se que seriam sujeitos a investigação com base numa mescla de informações concretas e abstractas" (PARECER..., 2008).

Segundo o Manual da Legislação Europeia sobre Protecção de Dados, são dados sensíveis:

> Quanto à definição de dados sensíveis, tanto a Convenção 108 (artigo 6.º) como a Diretiva de Proteção de Dados (artigo 8.º) identificam as seguintes categorias: • dados pessoais que revelem a origem racial ou étnica; • dados pessoais que revelem as opiniões políticas, as convicções religiosas ou outras; e • dados relativos à saúde e à vida sexual (MANUAL..., 2014).

Em sendo assim, revelar ou tratar dados, sem o consentimento do sujeito real, poderá importar ofensas ao corpo eletrônico. Importa destacar que dados aparentemente "inocentes", como alimentação em voos, manipulada para um determinado passageiro, pode revelar sua religião, bem como informações sobre alergias, podem indicar a presença de patologias. Tais dados, devidamente tratados, podem levar a um conhecimento iluminante sobre determinado sujeito, eventualmente sujeitando-o a exclusões discriminatórias.

a.3) Necessidade e Proporcionalidade

Em determinando momento, a AEPD assim refere: "É evidente o carácter intrusivo das medidas, como acima ficou indicado. Por outro lado, não está de todo demonstrada a sua utilidade." Portanto, uma enormidade de dados estava sendo transferido, mesmo em relação a pessoas sem qualquer envolvimento com grupos terroristas, e, como se vê, foram referidos como intrusivos e desprovidos de qualquer utilidade. Também, deve ser levado em conta que a entrega completa, enfim, de toda a lista de pessoas, implicaria em medida completamente desproporcional, como pontuado pela AEPD, pois permitiria um "controlo global das

deslocações de pessoas" (PARECER, 2008).

Logo, no sentir daquela Autoridade, tratar-se de uma situação que configuraria ofensa ao corpo eletrônico, por hiperexposição de dados.

b) Recomendação 2010/C 184 E/25

Trata-se de Recomendação do Parlamento Europeu ao Conselho, de 24 de Abril de 2009, referente ao problema da exploração de dados para a obtenção de perfis, nomeadamente com base na origem étnica e racial, nas operações de luta contra o terrorismo, manutenção da ordem, controlo da imigração, alfândegas e controlo fronteiriço. Na Recomendação constou que "a exploração de dados para a obtenção de perfis que tenha uma base especificamente racial ou étnica" suscita "profundas preocupações quando ao seu conflito com as normas da não discriminação[5]."

Nesta Recomendação, há uma classificação quanto aos perfis que se revela extremamente interessante, subdividindo-os em descritivos e preditivos.

> Considerando que os perfis podem ser:
> i) descritivos, quando têm por base testemunhos e outras informações acerca dos autores ou as características dos crimes cometidos, auxiliando, dessa forma, a apreensão de suspeitos específicos ou a detecção de actividades criminosas actuais que sigam o mesmo padrão; ou
> ii) preditivos, quando estabelecem correlações entre as variáveis observáveis de acontecimentos passados e os dados e informações confidenciais actuais, conduzindo a deduções que se crê passíveis de identificar aqueles que poderão estar envolvidos em crimes futuros ou ainda por desvendar (28), (PARLAMENTO EUROPEU, 2009).

Como se vê, em relação ao perfil preditivo, seria possível projetar a potencialidade de envolvimento em futuras práticas criminosas e, ferindo totalmente a presunção de inocência, por exemplo, tomar medidas preventivas para evitar o ingresso de estrangeiros em determinado país. A Recomendação também chamou a atenção para o sério problema de que "a prospecção de dados e a exploração de dados para a obtenção de perfis atenua a fronteira entre a vigilância orientada admissível e a problemática vigilância em larga escala", podendo

[5] Interessante notar que, do outro lado do Atlântico, na primavera de 2014 a Casa Branca divulgou um notável Relatório (que passou a ser chamado "Podesta Report", em razão do seu principal autor, John Podesta, então Conselheiro do Presidente Obama), em que se advertia expressamente "Big data can discriminate". Nesse relatório, afimou-se que sistemas de inteligência artificial tinham o potencial de exacerbar as desigualdades, por vezes de modo totalmente não intencional, vindo a afetar negativamente relações de locação, crédito, emprego, saúde, educação e mercado (BEDOYA, 2018, p. 232).

“conduzir a uma ingerência ilícita na reserva da intimidade da vida privada”

Logo, a Recomendação em comento, aponta a potencial utilização de dados sensíveis, registrando elementos, portanto, que revelam ofensa ao corpo eletrônico.

c) Processo C-210/16

Trata-se de pedido junto ao Tribunal de Justiça da União Europeia para desativar “fanpage”, uma vez que houve coleta de dados tanto pelo Facebook como pelo administrador da página, sem o devido consentimento. Foi estabelecida uma responsabilidade conjunta de ambos, tendo em vista o fenômeno denominado “*webtracking*”,

> que consiste em observar e em analisar os comportamentos dos utilizadores da Internet para fins comerciais e de marketing. Este webtracking permite nomeadamente identificar os centros de interesse dos utilizadores da Internet a partir da observação dos seus comportamentos de navegação. Fala-se então de «webtracking comportamental». Este último é feito geralmente através da utilização de cookies (PROCESSO..., 2017).

No caso, o Facebook e o administrador tomaram decisões quanto ao tratamento, já que “as estatísticas são elaboradas pela Facebook e personalizadas pelo administrador de uma página de fãs com a ajuda de diversos critérios que podem selecionar, como a idade e o sexo”. Portanto, ambos foram responsabilizados pelos danos cometidos aos usuários, tratados como “responsáveis”, o que na recente Lei Geral de Proteção de Dados Brasileira seriam definidos como “controladores”, em face de tomarem decisões, não se limitando ao tratamento. Nesse sentido, em nível de direito europeu, verifica-se uma miríade de ofensas ao *profiling*, que, em última análise, é o corpo eletrônico.

Identificadas as diversas formas pelas quais nosso corpo eletrônico pode sofrer ofensas, cumpre analisar, agora, quais as potenciais reações do ordenamento jurídico, com foco especialmente na responsabilidade civil.

3 REFLEXÕES ACERCA DA RESPONSABILIDADE POR DANOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA E A VIABILIDADE DA APLICAÇÃO DE DANO ESTÉTICO AO MUNDO DIGITAL

Esse capítulo está dividido em duas partes. Na primeira, tecemos algumas considerações sobre a responsabilidade civil em geral, à luz da recente normativa brasileira

que disciplina a proteção e dados. Na segunda parte, trataremos especificamente da possibilidade de se aplicar, ao mundo digital, as noções pertinentes ao dano estético.

3.1 REFLEXÕES ACERCA DA RESPONSABILIDADE POR DANOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA

A experiência europeia que, desde 1995, já contava com Diretiva própria de proteção de dados (Diretiva 95/46/CE), e que atualmente se encontra sob a égide do Regulamento Geral de Proteção de Dados, comprova que os danos atingem o corpo eletrônico e se projetam para o mundo físico.

Os algoritmos que são utilizados na construção do *profiling* consituem "blackbox", ou seja, verdadeiras "caixas-pretas", podem gerar danos ao se valerem de erros estatísticos, dados equivocados ou inverídicos, generalizações, uso de informações sensíveis ou correlação inadequada. O resultado disso afeta negativamente o corpo eletrônico do usuário.

Em caso recentemente levado ao Poder Judiciário brasileira, Recurso Repetitivo sob o nº 1.457.199/RS, Tema 710, junto ao Superior Tribunal de Justiça, a questão da formação de perfis comportamentais foi objeto de aprofundado estudo, na área das instituições financeiras, como relata Mendes (2014, p. 56):

> A falta de transparência dos sistemas de avaliação de risco é um dos principais problemas enfrentados não apenas por consumidores, mas também por reguladores e advogados. A obscuridade de diversos sistemas de avaliação de risco ensejaram a equiparação do *scoring* a uma "blackbox", dado que os processos pelos quais o histórico de crédito é convertido em um índice objetivo de risco são completamente intransparentes para um observador externo.

Exemplifica Mendes (2014, p. 114-115) que, através da utilização de "dados de geolocalização", como o "local de moradia", para formação do perfil do usuário, pode o algoritmo concluir que se o usuário mora em um determinado CEP onde residem pessoas com nível alto de inadimplência, mesmo que o usuário seja ótimo pagador, através de técnicas preditivas, poderá ser projetado como um golpista, equipara a descumpridor das obrigações, gerando um efeito desastroso na vida social e profissional do utente. Em sendo assim, ao escolher um local para morar, as pessoas teriam que, além de levar em consideração aspectos como localização, proximidade dos pontos de interesse pessoal, segurança, pesquisar também a vida financeira de seus potenciais vizinhos...

Ora, sem dúvida alguma, o mero *input* de dados, sem um filtro ético, nas mãos do

controlador e operador do tratamento de dados, pode levar a situações extremamente deletérias ao corpo eletrônico.

Na oportunidade da análise do ranqueamento do perfil comportamental bancário, o Ministro Paulo de Tarso Sanseverino, no julgado acima mencionado, assim se referiu quanto ao tratamento de dados, no Brasil:

> A vedação de utilização de dados sensíveis busca evitar a utilização discriminatória da informação, conforme claramente definido pelo legislador como aqueles "pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas." Desse modo, no sistema jurídico brasileiro, encontram-se devidamente regulados tanto o dever de respeito à privacidade do consumidor (v.g. informações excessivas e sensíveis), como o dever de transparência nessas relações com o mercado de consumo (v.g. deveres de clareza, objetividade e veracidade). Além disso, devem ser respeitadas as limitações temporais para as informações a serem consideradas, estabelecidas pelo CDC e pela Lei n. 12.414⁄2011, que são de cinco anos para os registros negativos (CDC) e de quinze anos para o histórico de crédito (Lei n. 12.414⁄2011, art. 14). No caso específico do "credit scoring", devem ser fornecidas ao consumidor informações claras, precisas e pormenorizadas acerca dos dados considerados e as respectivas fontes para atribuição da nota (histórico de crédito), como expressamente previsto no CDC e na Lei nº 12.414⁄2011. (BRASIL, 2014)

Como pedra de toque, no corpo da Lei Geral de Proteção de Dados brasileira, foi introduzido o direito à explicação, podendo o usuário requerer informações sobre como, através de algoritmos, enfim, do tratamento automatizado de dados, foi desenhado seu perfil, conforme se depreende dos termos dos parágrafos primeiro e segundo do mesmo artigo 20:

> § 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.
> § 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.

Além disso, introduziu, em nível legislativo, a definição de dados sensíveis, como se verifica no artigo 5º, II:

> 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;

E, de forma específica, estabeleceu as hipóteses do tratamento de dados sensíveis, que se restringe ao consentimento específico e às hipóteses legais exaustivamente apontadas:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Ademais, a Lei Geral de Proteção de Dados (LGPD) definiu regramento especial em matéria de responsabilidade civil, em razão do exercício da atividade de tratamento de dados pessoais, reconhecendo as espécies de danos indenizáveis. Segundo o *caput* do artigo 42 do referido diploma, literalmente, foram apontadas as seguintes modalidades de danos:

> 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 dados pessoais, é obrigado a repará-lo.

Como se verifica, a lei trata expressamente do dano patrimonial, que pode abarcar danos emergentes (o que efetivamente perdeu), bem como lucros cessantes (o que deixou de lucrar). Outrossim, também se reconhece o dano moral, em face do desgosto, da depressão, humilhação, desprestígio, que pode atingir o titular dos dados, que tenha sofrido constrangimento ou situação vexatória. É interessante referir que, em razão de estar se tratando de dados pessoais, erros podem atingir grande gama de pessoas, de forma simultâneas, com micro lesões, razão pela qual reconhece o legislador a possibilidade do dano vir a ser tutelado de forma coletiva.

Ainda que o artigo 42 da LGPD não especifique o fundamento da responsabilidade do controlador e do operador, se subjetiva ou objetiva, não parece haver margem para dúvidas no sentido de que se trata de responsabilidade objetiva. Ao não fazer menção a culpa, em sentido lato ou estrito, a moderna técnica legislativa está apontando para a responsabilidade objetiva. E isso fica claro a partir de uma interpretação sistemática, especialmente diante da

redação do art. 43 da LGPD:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Ora, se os agentes só não serão responsabilizados nestas hipóteses, significa que poderão afastar sua responsabilidade simplesmente alegando e provando não terem agido com culpa.

Trata-se da mesma técnica adotada, por exemplo, pelo legislador do CDC, ao disciplinar a responsabilidade do fabricante e do fornecedor de serviços pelo fato do produto ou do serviço (artigos 12, §3º e 14, §3º), sendo inequívoco que referidos dispositivos adotam a responsabilidade objetiva.

Controlador, segundo o artigo 5º, VI, é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;", enquanto o operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;", conforme dispõe o inciso VII do mesmo dispositivo. Como exemplo, pense-se na hipótese de um empresário do setor de venda de pizzas que determine a um serviço de atendimento online terceirizado, envolvendo nuvem (armazenamento de dados), que forme um cadastro, coletando dados, inclusive, relativamente à religião e saúde de seus consumidores, permitindo a geração de relatórios, com análises comportamentais. Neste caso, o dono do comércio de pizzas é o controlador, visto que toma as decisões de como será feito o tratamento, e, quais os dados devem ser coletados/tratados (no caso, a fim de futura transferência a farmácias ou a planos de saúde), e, o serviço de atendimento online, configura-se o operador, dado que apenas executa o tratamento em nome do controlador. Outro exemplo, está no Parecer 1/20 do "Grupo de Trabalho de Protecção de Dados do Artigo 29":

> A empresa ABC celebra contratos com diversas organizações para levar a cabo as suas campanhas de marketing directo e para gerir o processamento salarial dos seus funcionários, emitindo instruções específicas (que material de marketing enviar e para quem, a quem pagar, que montantes, até que data, etc.). Embora as organizações tenham alguma discricionariedade (nomeadamente quanto ao software a utilizar), as suas tarefas estão definidas de forma clara e rigorosa e, embora o operador de recolha e distribuição postal possa fornecer conselhos (por ex., aconselhando a não enviar mailings durante o mês de Agosto), está claramente obrigado a actuar de acordo com as instruções da ABC. (PARECER..., 2010).

Seguindo a análise, incumbe referir o disposto no parágrafo primeiro, do artigo 42 da Lei Geral de Proteção de Dados, que estabelece a responsabilidade solidária entre controlador e operador, quando houver descumprimento da lei, ou, ainda, não tiver o operador seguido as instruções lícitas do controlador:

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Convém destacar, por último, que o artigo 5º, VIII, da Lei sob o nº 13.709 de 2018, prevê a existência de um encarregado pela proteção de dados, que, conforme conceitua a legislação, é a "pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;". Importa referir, ainda, que a legislação estabelece as obrigações do encarregado, nos termos do artigo 41, § 2º:

> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Tendo em vista o encarregado não constar expressamente do artigo 42 da LGPD, aplica-se a responsabilidade subjetiva, somente respondendo civilmente quando agir com imprudência, imperícia e negligência, nas suas tarefas acima elencadas. É hora, agora, de enfrentar o questionamento final do presente estudo: No caso de ofensa ao perfil do usuário, poder-se-ia vislumbrar um dano estético digital?

3.2 VIABILIDADE DA APLICAÇÃO DE DANO ESTÉTICO AO MUNDO DIGITAL

Transpor o dano estético do mundo físico à dimensão virtual requer compreender em quais hipóteses o corpo de compleição concreta é objeto da violação e projetá-las sobre a corpulência binária formada por dados ligadas a uma pessoa natural. Segundo José de Aguiar Dias (1987, p. 868), a alteração do aspecto estético pode acarretar maior dificuldade no

granjeio da subsistência, diminuir as suas probabilidades de colocação ou exercício da atividade a que se dedica, sendo dessa natureza o dano estético que deforme desagradavelmente as feições, de modo que cause repugnância ou ridículo, e, portanto, dificulte a atividade da vítima.

Ora, a partir de uma dimensão digital, não é isto o que ocorre quando um perfil comportamental é erigido de forma equivocada ou em ofensa à Lei Geral de Proteção de Dados ou mesmo à sua principiologia? Eventualmente do evento danoso não poderia decorrer uma exposição à repugnância ou ao ridículo, dificultando, portanto, a existência da vítima?

O inadequado tratamento de dados, atingindo o *profiling* da pessoa natural, seja pela questão de erro estatístico, do equívoco de correlação (MENDES, 2018), de fato inverídico, ou, mesmo, a utilização de dados sensíveis, sem autorização, importará em ranqueamento desfavorável do usuário, em prejuízo de sua aparência binária, que estará comprometida, seja pela repugnância ou por cair no ridículo. Por exemplo, a indevida transferência de dado sensível por parte de um estabelecimento de saúde, a hipótese de ser portador de uma doença infectocontagiosa, para empresa de outro ramo, como do setor de seguros, ou, quem sabe, uma plataforma de emprego, gerará a desqualificação, alteração de degrau de ranqueamento relativamente ao seu perfil comportamental, e, em muitos casos, de forma permanente, causando-lhe um dano que vai além do episódico dano de ordem moral, evoluindo para um dano estético. As feições digitais da pessoa ficarão marcadas, dificultando a sua relação social, prejudicando-o em laços de amizade e vínculos profissionais.

Nos ensinamentos de Gustavo Borges (2014, p. 29), o dano estético "implica em uma modificação na aparência externa da pessoa", "que têm como marca a permanência, e causa uma espécie de 'enfeamento" na vítima. No mesmo sentido, Teresa Ancona Lopez (2004, p. 46) refere que dano estético envolve "qualquer modificação duradoura ou permanente na aparência externa de uma pessoa, modificação essa que lhe acarreta um 'enfeamento' e lhe causa humilhações e desgostos, dando origem, portanto, a uma dor moral". E, no caso concreto, a aparência do corpo eletrônico será diretamente afetada, de forma permanente, eis que lançada no mundo digital, enfeando o titular dos dados, refletindo em suas opções no mundo social e do trabalho. Saliente-se que o dano moral puro está relacionado a sensações[6] de dor, sofrimento, angústia, em face de uma exposição, que gera ao sujeito depressão, tristeza profunda, sob o viés estritamente subjetivo, enquanto a ofensa ao corpo eletrônico, atingindo o perfil comportamental, desborda para o dano estético, na medida em que terceiros,

[6] Lembrando-se que "estética" provém do grego *aisthesis,* que significa exatamente *sensação* (LOPEZ, 2004, p. 44).

que tomarem ciência do resultado algoritmo, que parte de erro, ou, exposição de dado sensível, tomarão decisões sobre a vida real do titular dos dados. Nesse contexto, o comando de "não colocar a mão sobre você" (RODOTÀ, 2005, p. 120-121), não se limita a não lhe agarrar um braço, ou lesionar, mas, também, não machucar sua dimensão digital (RODOTÀ, 2005, p. 120-121), seus dados pessoais.

Destaque-se que não se trata aqui da hipótese do mero vazamento de dados de uma imagem, que, por algumas horas, gera constrangimento à pessoa, e, nesse caso, seria objeto de dano moral contra aquele que tratou de forma inadequada sua imagem, mas a ofensa perene ao seu perfil comportamental, que lhe afastou e segue afastando de oportunidades nas relações amorosas, de amizades e do mundo do trabalho. É bem verdade que, se uma imagem for alvo do fenômeno da viralização, ou seja, com incontáveis compartilhamentos, também se poderá enxergar uma grave cicatriz no corpo eletrônico da pessoa natural, quando, também é possível, dada a ofensa que se prolonga no tempo, reconhecer o dano estético, além do dano moral. A viralização da imagem integrará inexoravelmente o perfil comportamental da pessoa, diante da coleta e tratamento dos gostos e geolocalizadores, sua viralização importará em impactos diretos em seu *profiling.* Neste caso, como já referido haverá consequências em seu campo profissional e social, sendo estes elementos de permanência, de continuidade de ofensa ao seu perfil, as hipóteses configuradoras de violação ao corpo eletrônico.

Ademais, importa destacar que a responsabilidade civil, em matéria de tratamento de dados, não se limita a danos de ordem material e moral, ainda que no *caput* do artigo 42 da LGPD somente tenha se referido a estes. Há muito que a doutrina mais crítica aponta para a vantagem de interpretar a legislação como se referindo não à visão simplista que divide os danos em materiais e morais, mas sim em materiais, de um lado, e imateriais ou extrapatrimoniais de outro, sendo este último um gênero que se subdivide em outras espécies de danos que nem sempre exigem a dor, sofrimento, angústia, como elementos caracterizadores (somente os danos morais puros exigiriam tais sentimentos). Dentro dessa categoria mais ampla de danos extrapatrimoniais, estariam incluídos, então, os danos estéticos, os danos psíquicos, os danos à honra, à imagem, à privacidade, bem como também os danos existenciais (recentemente positivados na reforma trabalhista), os danos ao projeto de vida, os danos à identidade, etc. Vários desses tipos de danos são corriqueiramente aplicados pela jurisprudência, ainda que sem previsão legal, já que o nosso sistema jurídico segue o modelo francês da atipicidade, em que o legislador apenas faz menção a "dano", sem especificar seu conceito e requisitos. Cabe à doutrina e à jurisprudência completar a obra do legislador nesse aspecto, como há mais de duzentos anos acontece com o direito francês e

como também vem ocorrendo conosco. Ora, de tal arte, como se vê, a Lei Geral de Proteção de Dados não obstaculiza o reconhecimento de dano estético, uma noção bem assentada em nossa doutrina e em nossa jurisprudência. Nesse sentido, compreende-se aplicável o dano estético ao mundo digital, ofensa ao corpo eletrônico, na medida em que "deforme desagradavelmente as feições (= à forma pela qual nos apresentamos e somos identificados no mundo virtual), de modo que cause repugnância ou ridículo, e, portanto, dificulte a atividade da vítima", causando restrições e dificuldades às tarefas que a vítima se dedique.

4 CONSIDERAÇÕES FINAIS

A partir do estudo realizado, tornou-se possível tecer as seguintes considerações finais, a saber: A uma, da formação de perfis comportamentais resulta a inequívoca dimensão do corpo eletrônico; A duas, resta possível identificar inúmeras ofensas ao *profiling*, que, em última análise, é o próprio corpo eletrônico; A três, os algoritmos, que são utilizados na construção do *profiling*, configuram-se, na maioria das vezes, uma "*blackbox"*, ou seja, verdadeiras "caixas-pretas", podendo gerar danos, ao se valerem de erros estatísticos, generalizações, uso de informações sensíveis ou correlação inadequada. O mesmo se opera pela utilização de dado inverídico ou que não esteja relacionado à pessoa natural do usuário, descaracterizando sua dimensão digital; A quatro, a responsabilidade do controlador e do operador é objetiva, enquanto a responsabilidade do encarregado é subjetiva; A cinco, o inadequado tratamento de dados, atingindo o *profiling* da pessoa natural, importará em ranqueamento desfavorável do usuário, em prejuízo de sua aparência binária, que estará comprometida, ceifando, ou preterindo, quando do oferecimento de bens ou serviços, que sequer poderá o usuário estimar, causando-lhe um dano que vai além do episódico dano de ordem moral, desbordando para um verdadeiro dano estético no mundo virtual. O estudo que se apresenta tem óbvia pretensão provocativa, desejosa de iniciar um debate, para o qual se convida o leitor a estar aberto para redefinir suas reflexões, adaptando-as para o mundo digital onde cada vez mais, querendo ou não, somos chamados a viver.

REFERÊNCIAS

BEDOYA, Álvaro M. Algorithmic Discrimination vs. Privacy Law. In: SELINGER, Evan; POLONETSKY, Jules; TENE, Omer (ed.). **The Cambridge Handbook of Consumer Privacy.** New York: Cambridge University Press, 2018.

BORGES, Gustavo. **Erro médico nas cirurgias plásticas**. São Paulo: Atlas, 2014.

BRASIL. Superior Tribunal de Justiça. **REsp. 1.457.199/RS.** Relator: Ministro Paulo de Tarso Sanseverino. Julgado em: 12 nov. 2014. Disponível em: <https://ww2.stj.jus.br/processo/pesquisa/?termo=1.457.199&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO>. Acesso em: 2018.

DIAS, José de Aguiar. **Da Responsabilidade Civil.** Rio de Janeiro: Forense, 1987. v. 2.

DONEDA, Danilo (2006). **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

_____. **Palestra em curso sobre a nova lei de proteção de dados**, em 29 de agosto de 2018, IDP/SP – ITS/RIO, 2018.

FAZENDEIRO, Ana. **Regulamentação geral sobre a proteção de dados.** Coimbra: Almedina, 2017.

FINOCCHIARO, Giusella. **Privacy e protezione dei dati personali:** disciplina e strumenti operativi. Torino: Zanichelli, 2012

GAUDENZI, Andrea Sirotti. **Diritto all'oblio: responsabilità e risarcimento del danno.** Santarcangelo di Romagna: Maggioli, 2017.

IGO, Sarah E. **The Known Citizen:** a history of privacy in modern America. Cambridge: Harvard University Press, 2018.

LOPEZ, Teresa Ancona. **O dano estético.** São Paulo: Revista dos Tribunais, 2004.

MANUAL da legislação europeia sobre proteção de dados. 2014. Disponível em: <fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>. Acesso em: 2018.

MAYER-SCHÖNBERGER, Viktor. **Delete:** the virtue of forgetting in the digital age. New Jersey: Princeton University Press, 2009.

MENDES, Laura Schertel. **Palestra em curso sobre a nova lei de proteção de dados**, em 29 de agosto de 2018. IDP/SP – ITS/RIO.

_____. **Privacidade, proteção de dados e defesa do consumidor.** São Paulo: Saraiva, 2014.

NISSENBAUM, Helen. **Privacy in context:** technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

ORTIZ, Concepción Conde. **La protección de datos personales:** un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid: Dykinson, 2005.

PAESANI, Liliana Minardi. **Direito e internet: l**iberdade de informação, privacidade e responsabilidade civil. 5. ed. São Paulo: Atlas, 2012.

PARECER 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante. 16 fev. 2010. Disponível em: <https://www.gpdp.gov.mo/uploadfile/others/wp169_pt.pdf>. Acesso em: 2018.

PARECER 4/2007 sobre o conceito de dados pessoais. 2007. Disponível em: <https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>. Acesso em: 2018.

PARECER da Autoridade Europeia para a Protecção de Dados sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (Passenger Name Record — PNR) para efeitos de aplicação da lei. **Jornal Oficial da União Europeia,** 01 maio 2008. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52008XX0501(01)&rid=1>. Acesso em: 2018.

PARLAMENTO EUROPEU. **Recomendação ao Conselho, de 24 de Abril de 2009,** referente ao problema da exploração de dados para a obtenção de perfis, nomeadamente com base na origem étnica e na raça, nas operações de luta contra o terrorismo, manutenção da ordem, controlo da imigração, alfândegas e controlo fronteiriço (2008/2020(INI)) Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52009IP0314&from=PT>. Acesso: 2018.

PEREIRA, Alexandre Libório Dias. **Informático direito de autor e propriedade tecnodigital.** Coimbra: Coimbra, 2001.

PROCESSO C-210/16. 24 out. 2017. Disponível em: <http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d0f130da1a16899d5b734ffdb82df20c1b964fba.e34KaxiLc3eQc40LaxqMbN4Pb3qNe0?doclang=PT&text=&pageIndex=0&docid=195902&cid=1436926>. Acesso em: 2018.

RODOTÀ, Stefano (2012). **Il diritto di avere diritti.** Roma-Bari: Laterza, 2012.

_____. **Intervista su privacy e libertà.** Roma-Bari: Laterza, 2005.

SANTAELLA, Lucia. **Linguagens líquidas na era da mobilidade.** São Paulo: Paulus, 2011.

SILVA, Leandro Augusto; PERES, Sarajane Marques; BOSCARIOLI, Clódis. **Introdução à mineração de dados.** Rio de Janeiro: Elsevier, 2016.

SOLOVE, Daniel J. La persona digital y el futuro de la intimidad. In: POULLET, Yves; ASINARI, María Verónica Pérez; PALAZZI, Pablo (coord.). **Derecho à la intimidad y a la protección de datos personales.** Buenos Aires: Heliasta, 2009.

UNIÃO EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. **Jornal Oficial da União Europeia,** 04 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em 2018.

WALDMAN, Ari Ezra. **Privacy as trust:** information privacy for an information age. New York: Cambridge University Press, 2018.