II ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

JOSÉ RENATO GAZIERO CELLA

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

D597

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

Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Fabiano Hartmann Peixoto; José Renato Gaziero Cella – Florianópolis: CONPEDI, 2020.

Inclui bibliografia
ISBN: 978-65-5648-260-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito, pandemia e transformação digital: novos tempos, novos desafios?

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Governança. 3. Novas tecnologias. II Encontro Virtual do CONPEDI (2: 2020 : Florianópolis, Brasil).

CDU: 34

CONPEDI

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

II ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O II ENCONTRO VIRTUAL DO CONPEDI, ocorrido entre os dias 02 a 08 de dezembro de 20202, foi realizado exclusivamente a partir da utilização das novas tecnologias de informação e comunicação e recebeu a submissão de um grande número de qualificados trabalhos, gerando a necessidade de estruturação de 3 Grupos de Trabalhos (GTs) específicos para a temática Direito, Governança e Novas Tecnologias.

O Grupo de Trabalho Direito, Governança e Novas Tecnologias II, com apresentações e discussões ocorridas em 03 de dezembro de 2020, organizou seus trabalhos em três grandes blocos temáticos, recebendo trabalhos situados na sociedade informacional, que foi fortemente impactada pela situação de pandemia ocasionada pela Convid-19, com reflexos em especialidades e profissões jurídicas.

No primeiro bloco de trabalhos, discutiu-se sobre o enfrentamento da morosidade na resolução de conflitos, a necessidade de redução de custos e a possibilidade de novas tecnologias a favor do Judiciário. Além do acesso à justiça, a judicialização deve ser equilibrada com a duração razoável do processo. A dificuldade de interoperabilidade de sistemas também foi asseverada. Na mesma linha, foram discutidas as aplicações de ferramentas de vigilância informacional e combinação de dados pessoais em agências, indicando perfil de pessoa propensa a cometer fraudes. A transparência tomou centro das discussões. O bloco seguiu com a construção da relevância do consentimento, mas acompanhado de mecanismos de controle e proteção. Usando-se o exemplo da wikiditadura e os riscos criados ao sistema educacional, também se debateu a estrutura de poder criada em torno de administradores, burocratas, verificadores e outras figuras (geralmente anônimas), que têm poder e controle sobre a comunidade digital. A discussão do bloco abordou também o problema das fake news e o indissociável risco de banalização de tema tão complexo ligado a muitas variáveis, desde a deliberada desinformação até informação incompleta e todos os seus reflexos em termos de fragilização de liberdade e cidadania.

No bloco seguinte, tratou-se dos impactos de ferramentas tecnológicas na privacidade e personalidade das pessoas, colisões de direitos fundamentais, bem como os riscos envolvidos pelo poder gerado com o domínio de ferramentas e tecnologias. Por outro lado, aspectos de proteção de direitos e do incremento dos marcos regulatórios, em especial a LGPD, permitem avançar os estudos para desequilíbrios, interferências e vinculações de/com poderes

constituídos sobre a ANPD, que podem comprometer as diretrizes dos direitos protetivos. Novas experiências tecnológicas de comunicação e interação com crianças também foram objeto do bloco, especialmente com os riscos de revelações de segredos e quebra de privacidades em um ambiente jurídico orientado pelo princípio da proteção integral. A colisão de direitos fundamentais no âmbito digital também foi objeto de discussões, especialmente pela descrição da internet balancing formula e sua atribuição de pesos para orientar decisões. O bloco finalizou com a discussão sobre o direito de não ser lembrado digitalmente como expressão da própria dignidade da pessoa e da insuficiência de tecnologias para assegurar tal direito. Sobre direitos ainda se discutiu o papel do uso da inovação para o desenvolvimento de uma política de propriedade intelectual que envolva o setor público e o setor privado.

No último bloco, tendo como pano de fundo a Covid-19, constatou-se diversos impactos da tecnologia, tanto em trabalhadores invisíveis potencializados na sociedade da informação com profundas alterações nas relações de trabalho, como nas profissões jurídicas tradicionais. Houve a percepção que pelo uso de tecnologias ocorreram alterações e, por outro lado, há uma limitação do Estado para o estabelecimento de soluções, ao tempo e forma que compatibilizem-se proteções e inovações. No campo jurídico, discutiu-se como a advocacia 4.0 também recebe demandas de segurança combinadas com exigências de respostas mais rápidas e precisas. Há, além do cenário de pandemia, muito mais expectativas criadas pela tecnologia no mercado jurídico. Há também o surgimento de uma variada gama de atividades aos especialistas jurídicos para a compatibilização e crescimento do cenário de inovação tecnológica. Os impactos da Covid-19 na aceleração do movimento de transição digital e o desenvolvimento de referenciais e aplicações de inteligência artificial também foram tratados no GT II. Destacou-se, por fim, também, a relevância de pesquisas com levantamento de dados e referenciais da sociedade atual com forma de melhor percepção dos impactos positivos ou riscos apresentados pela utilização de tecnologias.

Os Coordenadores

Prof. Dr. Aires José Rover

Prof. Dr. Fabiano Hartmann Peixoto

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. José Renato Gaziero Cella

Nota técnica: Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias II apresentados no II Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 7.1 do edital do Evento, e podem ser encontrados na Revista de Direito, Governança e Novas Tecnologias. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

O RISCO ALGORÍTMICO COMO VIOLADOR DOS DIREITOS HUMANOS NO CONTEXTO DA VIGILÂNCIA INFORMACIONAL: UMA ANÁLISE DA EXPERIÊNCIA HOLANDESA – SYSTEM RISK INDICATION - SYRI

ALGORITHMIC RISK AS A VIOLATOR OF HUMAN RIGHTS IN THE CONTEXT OF INFORMATIONAL SURVEILLANCE: AN ANALYSIS OF THE DUTCH EXPERIENCE - SYSTEM RISK INDICATION - SYRI

Ana Cláudia Miranda Lopes Assis [1]
Gabrielle Bezerra Sales Sarlet [2]

Resumo

Investigação, mediante pesquisa explicativa, exploratória e bibliográfica, acerca das tecnologias disruptivas e pervasivas conhecidas como TICs e da experiência holandesa SyRI para, partindo da configuração do sistema protetivo de direitos humanos, especialmente no que toca à função de garantir a privacidade no contexto atual, apontar os novos sentidos e o alcance das vulnerabilidades na sociedade informacional e, nesse sentido, esboçar algumas pautas para a sua regulação, para além da proteção de dados pessoais, e, portanto, uma conformação com a proteção multinível da pessoa humana dentro e fora do ecossistema virtual/digital, sobretudo no que toca ao estado de vigilantismo.

Palavras-chave: Sociedade informacional, Dados pessoais, Autodeterminação informativa, Privacidade, Ciberdemocracia

Abstract/Resumen/Résumé

Research, through explanatory, exploratory and bibliographic research, on disruptive and pervasive technologies known as ICTs and the Dutch SyRI experience, starting from the configuration of the protective human rights system, especially with regard to the function of ensuring privacy in the current context, to point out the new directions and scope of vulnerabilities in the information society and, in this sense, to outline some guidelines for their regulation, beyond the protection of personal data, and, therefore, a conformation with the multilevel protection of the human person inside and outside the virtual/digital ecosystem, especially with regard to the state of vigilantism.

Keywords/Palabras-claves/Mots-clés: Information society, Personal data, Informative self-determination, Privacy, Cyberdemocracy

[1] Mestre em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR). Doutoranda da Pontifícia Universidade Católica do Rio Grande do Sul e Faculdade Católica de Rondônia – DINTER – PUCRS/FCR.

[2] Doutora em Direito na Universidade de Augsburg (Alemanha). Pós-Doutora em Direito na Universidade de Hamburgo (Alemanha). Pós-Doutora em Direito na Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

1 INTRODUÇÃO

A economia da atenção, o processo de algoritmização do cotidiano e o capitalismo de vigilância andam de mãos dadas no cenário atual em que se compreende o ser humano a partir da íntima relação do mesmo com as chamadas tecnologias da informação e da comunicação (TICs) que, indubitavelmente, marcam as diversas áreas de atuação que se tem noticia atualmente. De fato, o ser humano foi não somente tragado pela realidade contemporânea, mas pode ser igualmente apontado como uma espécie de artífice, vez que atua de modo frenético na manutenção e na expansão desse fenômeno cultural. A expressão do tempo e do espaço passaram, nesse sentido, por intensas alterações que, em outro giro, implicam em releituras das balizas e fronteiras sociais, mas, mais especificamente do próprio sistema jurídico e de suas condições de aplicabilidade para encetar um novo perfil do sujeito/cidadão digital.

Se, por um lado, as TICs parecem trazer novas oportunidades, inclusive para o solucionamento de problemas complexos que afligem a Humanidade desde sempre como a fome, por outro, emulam novas situações que ora replicam questões de desigualdade e de estigmatização, reproduzindo alguns esquadros socialmente cruéis, ora encetam desafios e, com isso, implicam novas pautas de resolução para conflitos jamais vivenciados. Trata-se de uma realidade permeada pela monetização dos dados pessoais que, em síntese, passaram a valer mais do que os ativos fósseis e que, destarte, se projetam em um prognóstico de futuro em que, na medida em que desvelam inúmeros riscos para a pessoa humana, reforçam a ideia de funcionalização do mercado e do próprio Estado em favor dela.

A investigação do estudo proposto perpassa pela análise da complexidade e da relevância do tema que envolve a utilização das novas tecnologias, e.g., *Big Data, deep learning* e mineração de dados (*data mining)* e, desse modo, das múltiplas formas de coleta, de análise, de vinculação, de anonimização e de pseudoanonimização dos dados, sobretudo quando se tem em mente os dados pessoais, o que será levada a efeito por meio da pesquisa exploratória, tendo como pano de fundo a decisão do Tribunal Distrital de Haia (Holanda), no Processo C-09-550982-EM ZA 18-388, que analisou a implantação de um Sistema de Indicação de Risco – *System Risk Indication – SyRI,* baseado na Lei de Organização de Implementação e Estrutura de Renda (*Wet structuur uitvoeringsorganisatie em inkomen – SUWI*[1]).

Importa mencionar que consiste em um projeto do governo holandês com a finalidade de prevenir e de combater as fraudes no domínio da seguridade social e dos regimes

[1] Em uma tradução livre-se, entenda-se Lei de Estrutura de Implementação de Trabalho e Renda.

relacionados com rendimento, impostos, contribuições e áreas ligadas à legislação laboral, sendo realizado por meio de um processamento de dados coletados por diversas autoridades públicas que, com base em um perfil de risco, indica probabilidades de fraudes por cidadãos que solicitaram os benefícios do Estado.

Quanto ao método e o procedimento utilizado para trabalhar a problemática proposta, optou-se pelo teórico e bibliográfico, cuja discussão perpassa por consultas em doutrinas e em legislações, sobretudo das que perfazem o sistema normativo da União Europeia - UE, para fins de alcançar a noção elementar apropriada aos novos contornos do direito à privacidade na Convenção Europeia de Direitos Humanos, de modo a contribuir em uma perspectiva integrativa para o delineamento de uma paleta de direitos e de garantias factíveis. Para tanto, deve-se sublinhar a relevância das investigações acerca do tensionamento entre a autodeterminação informativa e os diversos aspectos da sociedade plenamente ancorada no uso das TICs que, em síntese, traduz-se como um campo caracterizado pela erosão de alguns dos mais significativos pilares do Estado democrático de Direito.

Deste modo, por meio do método de interpretação qualitativa, de forma analítica e explicativa, procurou-se destacar os principais componentes da pesquisa relacionados ao tema geral que, além de envolver de modo especial as questões referentes ao direito à privacidade, enfrentou inclusive a problemática da discriminação e da estigmatização[2] no novo ambiente panóptico[3].

Justifica-se, por oportuno, a importância desse estudo de modo a propor novas pautas de soluções e de interpretações como forma de garantir a privacidade e, nesse sentido, combater a discriminação algorítmica, assim como as modalidades de interferência indevida na vida da pessoa humana por meio da captação e da análise de dados pessoais sem qualquer consentimento ou conhecimento daquela, em evidente contraposição às hipóteses legitimamente autorizadoras.[4] Ao final, serão analisados os efeitos deletérios da inobservância da autodeterminação informativa no contexto hodierno.

Nessa ordem, pretende-se registrar nos moldes científicos, a consonância do presente estudo com a linha de pesquisa relacionada no Edital nº 03/2020 do Conselho Nacional de

[2] Na identificação do termo vigilantismo (*surveilance),* Fernanda Bruno (2006) menciona ser instrumentalização do poder, via domínio sobre fluxos informacionais que são convertidos em conhecimentos capazes de permitir o controle social, tais como detecção de comportamentos suspeitos em imagens captadas por câmeras de segurança; avaliação de créditos em atividades financeiras, dentre outros.

[3] Vide artigo 39 do GDPR quanto as hipóteses que legitimam o processamento de dados pessoais. No mesmo sentido, tem-se o artigo 6º da Lei Nº 13.709, de 14 de agosto de 2018 (LGPD).

[4] Cf. Artigo 6º do GDPR que estabelece as situações de licitude do tratamento dos dados pessoais. No mesmo sentido, o artigo 7º da Lei Nº 13.709, de 14 de agosto de 2018 (LGPD).

Pesquisa e Pós-Graduação em Direito – CONPEDI, notadamente, no especificado na ementa "Direito, Governança e Novas Tecnologias", visto que por meio de uma análise crítica, vislumbra-se possibilidade de realizar o aprofundamento das temáticas que envolvem as novas tecnologias para fins de vigilância e o direito como instrumento capaz de superar as contradições de forma democrática e ampliar a proteção dos direitos fundamentais.

2 OS DIREITOS HUMANOS, O SISTEMA INTERNACIONAL DE PROTEÇÃO E O PAPEL DO SISTEMA REGIONAL EUROPEU

Ab initio destaque-se, por obvio, que a expressão "direitos humanos" se alicerça na sua relação com os instrumentos normativos de direito internacional que o reconhecem como tal (o fato de ser pessoa humana, traduzindo-se em direito de todos) no plano de validade universal, de modo a revelar o caráter supranacional desse direito (SARLET, 2018, p. 29). Trata-se, dessa maneira, de categoria fundante na medida em que introduz um sujeito de direito de caráter e de atuação internacional, independentemente do atributo da nacionalidade.

A Declaração Universal de 1948 introduziu a concepção contemporânea dos direitos humanos, reiterada em 1993 pela Declaração de Direitos Humanos de Viena, as quais apontaram a universalidade (extensão universal da condição de pessoa) e indivisibilidade desses direitos (englobando direitos civis, políticos, sociais, econômicos e culturais), com atributos interdependentes e inter-relacionais de amplo alcance, a enquadrá-los no constitucionalismo global, por compreender "o novo paradigma centrado nas relações Estado/povo, na emergência de um Direito Internacional dos Direitos Humanos e na tendencial elevação da dignidade humana a pressuposto ineliminável de todos os constitucionalimos" (PIOVESAN, 2017, p. 53), justificando a vinculação às regras e aos princípios de direito internacional protetivos.

O contínuo destaque aos Direitos Humanos impulsiona esforços que, por sua vez, implicam por parte do Estado e da própria sociedade, a implementação de novos instrumentos para fazer frente às atuais conjunturas, principalmente, "no momento em que os seres humanos se tornam supérfluos e descartáveis [...] em que é cruelmente abolido o valor da pessoa humana" (PIOVESAN, 2017, p. 51).

Assim, o Direito Internacional dos Direitos Humanos ganhou relevância com a Declaração Universal de 1948, conferindo uma concepção contemporânea desses direitos mediante uma série[5] de tratados e de instrumentos internacionais como forma legal de impor obrigações aos Estados (sentido amplo), quanto ao modo de agir de determinadas maneiras e

[5] As normas internacionais de direitos humanos consistem, principalmente, em tratados, costumes, declarações, diretrizes, princípios, dentre outros.

se absterem de certos atos, afetando, consequentemente, o próprio Direito Interno, já que a salvaguarda do "mínimo ético irredutível" (PIOVESAN, 2017, p. 55) não está adstrita ao alvedrio da competência nacional ou doméstica, eis que em prol dos direitos humanos, a soberania estatal não é absoluta, diante da legitimação alcançada pelo Sistema Internacional de Proteção[6], materializador da estrutura formal e material da jurisdição internacional.

O Sistema Internacional de Proteção dos Direitos Humanos se constitui em dois sistemas normativos que se complementam, o Global e o Regional. O sistema Global de Direitos Humanos corresponde ao da Organização das Nações Unidas, doravante ONU, que expressa os ideais e os propósitos dos povos dos Estados-Membros[7], possuindo supremacia no "caso de conflito entre as obrigações dos membros das Nações Unidas [...] e as obrigações resultantes de qualquer outro acordo internacional"[8], cuja organização interna encontra previsão no artigo 7º da Carta da ONU, sendo: Assembleia-Geral, Conselho de Segurança, Corte Internacional de Justiça, Conselho Econômico e Social[9], Conselho de Tutela e Secretaria.

Impende mencionar, contudo, que os documentos criados pelos órgãos da ONU, com base em convenções, declarações e recomendações, não denotam uma aplicabilidade imediata e direta capaz de integrar o ordenamento jurídico dos Estados-Membros, assim como não são capazes de suscitar a revogação de normas implementadas por estes no caso de incompatibilidade com os atos normativos da ONU, levando ao reconhecimento quanto a inexistência da supranacionalidade da entidade.

Diante disso, considerando as características, as especificidades e os valores históricos e culturais dos povos de diferentes regiões do mundo, foi instituído os Sistemas Regionais de Proteção dos Direitos Humanos que, de fato, abarcam grupos de países regionalmente limítrofes, sendo encontrados em funcionamento os sistemas europeu, o interamericano e o africano, assim como os novos sistemas asiáticos e árabe, os quais, contudo, não possuem a mesma medida de implementação[10] dos mais antigos.

---

[6] A título exemplificativo o Pacto Internacional dos Direitos Civis e Políticos, A Convenção sobre a Discriminação Racial; A Convenção sobre a Eliminação da Discriminação contra a Mulher, Convenção sobre os Direitos da Criança etc.

[7] A ONU foi fundada em 24 de outubro de 1945, com membros de todos os cantos do planeta, sendo definido a comunicação entre eles em seis idiomas oficiais, quais sejam: inglês, francês, espanhol, chinês e russo. Em 1973 inclui-se como idioma oficial o árabe.

[8] Cf. Artigo 103 da Carta das Nações Unidas.

[9] Considerado o órgão da ONU que detém maior importância em razão da competência em promover a cooperação de questões econômicas, sociais e culturais, relacionados aos direitos humanos.

[10] Cf. Flávia Piovesan, "muitas lideranças asiáticas têm expressado ceticismo quanto aos direitos humanos, visto como uma agenda neocolonizadora do mundo ocidental" (2017, p. 109) e, em relação ao sistema regional árabe, submete a interpretação à lei da Sharia, consoante artigo 25 da Declaração do Cairo dos Direitos Humanos, contradizendo o discurso universalista da Carta Árabe dos Direitos Humanos.

Cada sistema regional possui o seu ordenamento jurídico próprio, merecendo destaque pela proposição do presente estudo, o europeu, o mais consolidado e com forte influência nos demais, que surgiu em razão de um contexto de ruptura do final da 2ª Guerra Mundial, ou seja, como oposição ao cenário dos horrores e das atrocidades cometidas em desrespeito à dignidade da pessoa humana, de modo a significar, de acordo com Flávia Piovesan o "marco do processo de integração europeia e da afirmação de valores da democracia, do Estado de Direito e dos direitos humanos" (2017, p. 119).

A Convenção Europeia para a Proteção de Direitos Humanos e das Liberdades Fundamentais, também conhecida pela expressão abreviada de Convenção Europeia dos Direitos do Homem, doravante CEDH ou Convenção, objetivou unificar a Europa e assegurar a promoção e a proteção de pessoas que se encontrem no território europeu (em razão do seu alcance amplo) dos direitos e das liberdades contidos na Convenção, tais como direitos civis, culturais, econômicos, políticos e sociais, estando os Estados-partes ratificadores obrigados a observarem os parâmetros ali contidos, o que implica na compatibilização dos respectivos normativos internos, consoante previsão contida no artigo 52 da Convenção.

Frise-se que os princípios da solidariedade e subsidiariedade, vetores dessa normativa, denotam o compromisso dos Estados-partes na observância da CEDH, que possui atuação subsidiária na complementação dos regramentos internos, considerando as transformações nos planos social e político e no panorama das realidades contemporâneas, como forma de alcançar os objetivos propostos para salvaguardar os direitos humanos.

As decisões do Sistema Regional têm impactado consideravelmente as legislações e a prática de atos violadores dos direitos humanos dos Estados-parte, cujos direitos reconhecidos na CEDH foram se desvelando em um contexto temporal e social, ante o crescente nível de exigência em matéria de direitos humanos e de liberdades fundamentais que reclamam proteção, como é o caso dos direitos à privacidade, igualdade (não-discriminação) e proteção de dados pessoais.

Portanto, a fim de promover a harmonização dos diversos regimes jurídicos de direitos humanos vigentes nos Estados-parte da Convenção, por meio de uma interpretação evolutiva vislumbra-se a possibilidade de progredir na verificação da garantia maior de proteção, ampliando-se o campo de aplicação dos direitos definidos no artigo 8º da Convenção, de modo a confirmar sua evolução, o que tem sido motivo de insistência pelo Parlamento Europeu quanto a necessidade de se alcançar um equilíbrio entre melhoria da segurança e a preservação dos direitos humanos, incluindo a privacidade e proteção de dados. Assim, em maio de 2018

entraram em vigor novas regras da União Europeia em matéria de proteção de dados, reforçando os objetivos da CEDH, tema que será exposto nos tópicos subsequentes.

3 RISCO ALGORÍTMICO NA DETECÇÃO DE FRAUDE PREVIDENCIÁRIA NA HOLANDA

O *SyRI* (*System Risk Indication*) consiste em uma ferramenta digital utilizada pelo Ministério Holandês de Assuntos Sociais e Emprego para prevenir e combater o uso ilegal de recursos públicos, evitar fraudes tributárias na previdência social e violações às leis trabalhistas. Essa medida foi estabelecida a pedido de agências e de órgãos públicos, diante da detecção de elevado número de fraudes contra a fazenda pública, sendo então projetada pelo governo holandês que, por meio da combinação de amplas categoriais de dados previamente armazenados separadamente por instituições públicas, são analisados por um modelo de risco algorítmico não divulgado que indica perfil de risco de pessoa propensa a cometer fraudes. Desde sua implantação, o referido sistema foi exclusivamente utilizado em áreas com alta proporção de residentes de baixa renda, imigrantes ou minorias étnicas.

Apelidado pelos defensores de direitos humanos de "estado de vigilância do bem-estar" (*welfare surveillance state*), o *SyRI* faz parte de uma tendência global de introdução de ferramentas digitais que desconsideram as consequências potencialmente devastadoras de direitos protegidos internacionalmente, tais como o direito à privacidade, proteção de dados e seguridade social.

Por representar um risco ao Estado Democrático de Direito e violação de direitos fundamentais foi proposta uma ação por uma coalização de ONGs na defesa direitos humanos e direitos digitais, incluindo o *Public Interest Litigation Project*[11] e *Privacy First*[12] para bloquear a implantação do *SyRI,* visto constituir-se em um sistema de detecção digital direcionado que classifica cidadãos em um perfil de risco por meio da utilização da mineração de dados, baseado na vinculação automatizada em larga escala, não estruturada e sem foco dos arquivos de pessoas com características específicas, assim como *deep learning,* referente a uma configuração de parâmetros básicos de dados obtidos de múltiplas camadas de processamento para auxiliar o algoritmo a desenvolver uma classificação e descrever um conteúdo ou perfil, por meio do processamento secreto de dados pessoais, o que também poderia ocasionar tomada

[11]Pertencente à organização da Seção Holandesa da Comissão Internacional de Juristas (NJCM) que objetiva proteger minorias vulneráveis e fornecer acesso à justiça. Revisa a conformidade na implantação de novas políticas e propostas legislativas aos padrões de direitos humanos estabelecidos em tratados internacionais e europeus.

[12] Fundação independente de interesse coletivo com objetivo de preservar e promover o direito à privacidade.

de decisão individual automatizada. Foi sustentado ainda o enquandramento do *SyRI* no *Big Data* (megadados), diante do grande volume de dados em vários formatos (estruturados e não estruturados), oriundos de sistemas gerenciadores de banco de dados de diversas organizações que criam conexões entra elas para fins de identificação do perfil de risco, motivando o pedido de não vinculação daquele sistema na tomada de decisão, por se tratar de uma invasão não autorizada da privacidade e não possuir garantias suficientes à proteção de dados.

Em defesa, o governo holandês sustentou a adoção de critérios objetivos com garantias processuais e materiais, sendo utilizados dados dos órgãos previstos na Lei de Organização de Implementação e Estrutura de Renda (*SUWI*), que autoriza a preparação de relatórios de risco para avaliar a probabilidade de uma pessoa física ou jurídica fazer uso ilegal de fundos governamentais no campo da previdência social e esquemas relacionados à renda pública, cujas informações seriam comparadas e avaliadas para verificar discrepâncias entre elas e, se constatadas, realizar-se-ia uma investigação mais detalhada antes da tomada de decisão, refutando a alegação da aplicação do *deep-learning* e da análise preditiva do sistema.

Ao analisar a ferramenta *SyRI,* o Tribunal Distrital de Haia (*Rechtbank Den Haag)* inicialmente avaliou o quadro geral de implicações aos direitos humanos na CEDH (Lei 16/1950), que estabelece em seu artigo 8º, 1, o direito ao respeito pela vida privada e familiar: «Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência, uma vez que os Países Baixos estão vinculados pela Convenção à jurisdição do Tribunal Europeu dos Direitos do Homem (TEDH)[13], que consagrou importantes parâmetros acerca da vida privada, contemplando a proteção ao direito à autonomia, ao desenvolvimento e ao autodesenvolvimento pessoal, assim como o direito de estabelecer um relacionamento com os outros e com o mundo exterior, ou seja, trata-se de elementos que perfazem o princípio da dignidade e, assim, alicerçam o direito da liberdade humana pertencentes à própria essência da Convenção que, juntamente com a noção de autonomia pessoal, desempenham um papel de destaque na determinação do alcance do direito ao respeito pela vida privada.

Em decorrência do TEDH convém identificar o direito à identidade e ao desenvolvimento pessoal como aspectos parciais do direito ao respeito à vida privada, ressaltando-se que o direito à identidade pessoal se relaciona intimamente com o direito à proteção de dados pessoais, pois, no caso do processamento sem justificativa plausível e sem

[13] Cf. Art. 32 do CEDH: "A competência do Tribunal abrange todas as questões relativas à interpretação e à aplicação da Convenção e dos respectivos protocolos que lhe sejam submetidas nas condições previstas pelos artigos 33º, 34º, 46º e 47º".

consentimento motivado do titular dos dados, por certo, afeta o direito à igualdade de tratamento em casos iguais e o direito à proteção contra discriminação, estereótipos e estigmatização[14]. Assim, foi considerado que o direito à proteção de dados pessoais não se referia a um direito independente da CEDH, eis que de fundamental importância em sentido amplo para o respeito à privacidade.

Observou-se, ainda, as implicações no artigo 17 do Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, necessário em uma sociedade democrática em prol da segurança nacional, da segurança pública ou do bem-estar econômico do país, a prevenção de desordens, a proteção da moral, saúde e dos direitos e liberdades de terceiros, sendo ressaltado pelo Tribunal que o artigo 17 do Pacto Internacional[15] oferece a mesma proteção à vida privada que o artigo 8º (2)[16] da CEDH, por não possuir significação independente.

Embora tenha sido considerado pelo Tribunal Distrital de Haia que o quantitativo elevado de fraudes no sistema de previdência na Holanda justifique a aplicação de mecanismos de controle e supervisão para limitar e/ou eliminar aqueles problemas, vislumbrou-se um efeito significativo das indicações de risco na privacidade das pessoas "afetadas", mormente pela não observância aos princípios da transparência, da limitação da finalidade e da minimização dos dados, porquanto não ser aquele sistema suficientemente claro, de modo a não se enquadrar no escopo da proteção do artigo 8º (2) da CEDH, já que nos termos dos artigos 64 e 65 do *SUWI*[17], o fornecimento de dados entre instituições que possuem as informações pessoais caracteriza significativa interferência no direito ao respeito pela vida privada, ante a falta de transparência dos modelos e dos fatores de risco aplicados, possibilitando um efeito discriminatório e estigmatizante, na medida em que baseado no *status* socioeconômico das pessoas ou histórico de imigração.

---

[14] Neste ponto, toma-se o entendimento de Roger Raupp Rios, acerca do direito da antidiscriminação ter o "imprescindível compromisso com a afirmação do direito humano e constitucional de igualdade".

[15] Na identificação do objetivo do Pacto Internacional dos Direito Econômicos, Sociais e Culturais, adotado pela ONU em 1996, acerca da incorporação dos dispositivos da Declaração Universal como preceitos juridicamente obrigatórios e vinculantes, Piovesan (2010, p. 122), ressalta que o "intuito desse Pacto foi permitir a adoção de uma linguagem de direitos que implicasse obrigações no plano internacional, mediante a sistemática da international accountability.[...] ensejando a responsabilização internacional em caso de violação dos direitos que enuncia".

[16] O artigo 8º (2) da CEDH estabelece a possibilidade da ingerência no direito à privacidade somente quando houver previsão legal ou necessário à "segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção de infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros".

[17] Artigo 64 trata da prestação de informações em benefício de uma parceria, cujo parágrafo 1º e alíneas destacam os colaboradores para fins de ação governamental integrada em relação à prevenção e combate ao uso ilegal de fundos públicos, fraude fiscal e de prêmios e ao não cumprimento das leis laborais. Por sua vez, o Artigo 65 refere-se à indicação de risco do sistema (SYRI), cujo parágrafo 2º destaca que os dados referidos no primeiro parágrafo só podem ser utilizados para a elaboração de uma comunicação de riscos sobre uma pessoa singular ou coletiva. (tradução nossa).

Identificou-se, inclusive, ausência de publicidade e possível análise preditiva com vinculação automatizada em larga escala, não estruturada e sem foco, permitindo adaptação de um modelo de risco com base em reconhecimento de padrões, de modo a indicar a aplicação do *deep learning,* mineração de dados e ser o processamento de dados qualificado como *Big Data,* diante da grande quantidade de informações coletadas de diferentes fontes.

A decisão destaca também que o desenvolvimento de novas tecnologias deve obedecer o direito ao sigilo dos dados pessoais, cabendo aos Países Baixos, enquanto Estado-Membro da União Europeia, uma responsabilidade especial na sua aplicação, devendo ser encontrada uma relação ou justificativa razoável, como forma de ponderar o interesse social na prevenção e no controle e no respeito ao direito à privacidade. Ao final, foi destacado no julgado que a tomada de decisão individual automatizada afronta o artigo 22 do *General Data Protection Regulation* (GDPR), por traduzir uma espécie de interferência na vida privada das pessoas, sendo então declarado ineficaz a utilização daquele sistema.

Trata-se de uma decisão histórica na aplicação de padrões universais de direitos humanos como forma de lidar com os riscos dos sistemas emergentes de bem-estar digital, mormente quando a utilização de ferramentas do tipo *SyRI* estão se tornando uma tendência global[18] em direção à introdução e à expansão de tecnologias digitais em situações assistenciais, cujas consequências são potencialmente devastadoras para os direitos das pessoas mais pobres e marginalizadas, tal como o caso ocorrido no Estado de Wisconsin nos Estados Unidos da América que, por meio da avaliação de risco do COMPAS, estimava a probabilidade de reincidência criminal com base na análise de perfis idênticos, mesma faixa etária e ficha criminal, havendo diferenciação apenas na característica da cor, verificando-se maior probabilidade de um indivíduo negro receber pontuação mais alta do que o branco naquele perfil.

Inegável a utilização de ferramentas ou arranjos tecnológicos capazes de atuar como modelo de vigilância por meio do processamento de informações fornecidas pelo próprio cidadão que vem se tornando cada vez mais dependente dos meios tecnológicos, aumentando,

[18] A esse respeito, cita-se o plano anunciado em 2014 pelo governo chinês, com previsão de total implantação em 2020, quanto ao controle e prevenção de ações dos cidadãos chineses, baseado em um "sistema de ranking social" (*Social Score*), consistente em uma plataforma digital de avaliação por pontos que, de acordo com os hábitos de compra, entre outros dados, tais como número de identificação, código de crédito social unificado das empresas, informa as pontuações de estilo de crédito que estão vinculados às classificações do governo chinês e, com base na aceitação, reverte em melhores e mais condições de vida e negócios aqueles que obtiverem maior pontuação, em contrapartida, aos que ficarem com pontuação menor e que passam à condição de ostracismo e marginalidade, com indicação do nome em uma espécie lista negra.

em contrapartida, a acumulação e a circulação de dados[19] disponibilizados nas redes, tornando-os matérias-primas para tratamento e utilização aos mais diversos fins[20].

A identificação da forma como foram utilizadas as ferramentas tecnológicas indicadas na decisão da Holanda e a ausência de transparência nas justificativas da implementação do programa *SYRI*, permitem uma maior reflexão acerca das eventuais violações ao direito à privacidade, mesmo quando justificado o uso para interesses públicos, sendo imperioso registrar que aquele direito não deve ser entendido somente no aspecto individual, visto também referir-se a um bem coletivo[21] (direito à proteção de dados, acesso aos dados pessoais e *habeas data*), na medida em que normas, políticas públicas e empresariais possuem capacidade de afetá-lo, reforçando o entendimento quanto a autodeterminação informativa ser expressão da liberdade pessoal, com "status de direito fundamental" (DONEDA, 2006), cabendo-lhe a decisão de dispor de suas informações pessoais como bem entender. Assim, o direito à privacidade deve ser entendido como uma "espécie de 'imunidade' às trocas desconhecidas, indesejadas e não intencionais de informações" (COLOMBO, 2017).

4 NOÇÕES ELEMENTARES DO DIREITO À PRIVACIDADE NA CEDH, À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (GDPR)

Na União Europeia, o direito à proteção de dados, engloba as informações pessoais, caracterizados pela identificação do titular diretamente (CPF, Carteira de Registro Civil, nome, endereço etc), os dados sensíveis, decorrentes do cruzamento de dados (escolaridade, gênero, geolocalização, faixa etária) e os metadados (gerados pelos mais diversos dispositivos digitais que acrescem informações com objetivo de facilitar e evidenciar o titular), encontra guarida, principalmente, na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre Funcionamento da União Europeia, doravante denominado este último como TFUE, sendo estabelecido no artigo 7º da Carta que, todos têm direito ao respeito à vida privada, englobando a familiar, assim como a casa e as correspondências. O artigo 8º da Carta e artigo 16 da TFUE,

[19] A computação em nuvem (*cloud computing,* em inglês) possibilita acessar programas, arquivos e serviços por meio da internet, sem necessidade de estarem as informações armazenadas nos dispositivos pessoais de um indivíduo, já que os arquivos se encontram espalhadas em servidores virtuais, acessíveis em diversos locais, traduzindo-se tal serviço como mero armazenamento de informação.

[20] Exemplificando tem-se o compartilhamento das informações com empresas terceirizadas em diferentes aplicativos, bem como para finalidades legais, tal como a utilização do PJe com acesso via computação em nuvem com a utilização da infraestrutura do Conselho Nacional de Justiça.

[21] No caso *Halabi v. Estado Nacional,* julgado em 24.9.2009, pela Corte Suprema de Justicia de la Nación Argentina, declarou a inconstitucionalidade da Ley 25.873, de 2003, e sua regulamentação (determinava o armazenamento obrigatório de dados por 10 anos pelas empresas de telecomunicação, com a finalidade de serem utilizados para fins probatórios em processos judiciais), foi demonstrado que o direito à privacidade refere-se tanto a um bem individual quanto coletivo.

declaram ainda o direito à proteção dos dados pessoais, bem como a necessidade de haver um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou em razão de alguma outra base legítima estabelecida por lei, consoante prevê o artigo 8º da Carta.

Pelo fato do tratamento de dados pessoais se referir a um direito fundamental essencial ao livre desenvolvimento humano, e com o fim de reforçar a privacidade dos cidadãos no território da União Europeia, em abril de 2016 foi aprovado pelo Conselho Europeu o Regulamento Geral de Proteção de Dados (RGPD)[22], tradução de *General Data Protection Regulation* (GDPR), que estabelece regras quanto ao tratamento, por pessoa, empresa ou organização, de dados pessoais na União Europeia, sendo executável a partir de 25 de maio de 2018**,** diante da necessidade de um período de dois anos para adequação às mudanças implementadas. Mencionado regulamento é aplicável a todos os Estados Membros da União Europeia, eis que vinculativo a qualquer organização que ofereça bens ou serviços que coletem dados pessoais relacionados àquele bloco.

O GDPR objetiva reforçar e unificar a proteção de dados pessoais, adaptando seus princípios a um mundo cada vez mais dependente da coleta e do tratamento desses dados na *internet* e fora dela, tendo substituído a antiga Diretiva 95/46, do Conselho Europeu de 1995, implementada para garantir aos cidadãos europeus o direito à autodeterminação informativa (*Grundrecht auf informationelle Selbstbestimmung*), ou seja, o direito de saber como e para qual finalidade seriam utilizados seus dados e, dessa forma, decidir em que medida poderia ter suas informações publicadas e/ou processadas, sob pena de afronta direta ao direito fundamental da privacidade.

Tem-se, assim, o fortalecimento do direito à proteção de dados pessoais e dos requisitos para o consentimento quanto a coleta e tratamento das informações, passando aquela autorização a figurar como um elemento principal, que deve ser inequívoca e envolver uma postura assertiva para não resultar na responsabilização daqueles que realizarem a coleta inadequadamente (artigos 6, 7 e 8 do GDPR). Enfatize-se a obrigação do responsável pelo tratamento dos dados levar em conta a probabilidade e a gravidade dos riscos aos direitos e liberdades das pessoas quando do processamento de dados (artigo 24). Esclareça-se, ainda, que as situações de necessidade do consentimento livre e informado[23] guardam estreita correlação com o princípio da transparência, assim como não descarta a possibilidade de revisão e retirada

[22] Considerado uma reação à espionagem em massa promovida pelos governos dos Estados Unidos da América, em razão do compartilhamento de informações digitais com outros países, tais como o Reino Unido.

[23] Sobre o tema, o artigo 12 da GDPR estabelece os requisitos de um consentimento informado do titular para o processamento dos dados.

da anuência, a qualquer tempo e sem prejuízo da não divulgação dos dados (SARLET; CALDEIRA, 2019).

Ademais, a CEDH prevê uma proteção mínima do direito ao respeito pela privacidade, cujo conteúdo e o alcance dos direitos fundamentais são os mesmos contidos na Carta dos Direitos Fundamentais da União Europeia, eis que correspondentes (artigo 52, item 3 da Carta), todavia, a proteção dos dados pessoais na Carta vai além do previsto na CEDH. Nem por isso, é sustentada uma posição preferencial em abstrato para algum direito previsto em qualquer uma delas, vez que cautelas e limites às restrições devem obedecer ao critério da proporcionalidade dos direitos fundamentais em geral, em razão do conceito multidimensional desses direitos, de modo que a aplicação dos princípios indicados no GDPR enseja observância àqueles direitos, bem ainda aos direitos sociais, juntamente com o enfoque voltado para a proteção do interesse público.

Dentre os princípios garantidores no GDPR destacam-se o da licitude, da lealdade e da transparência; da adequação e da limitação da finalidade; da necessidade ou da minimização dos dados; da qualidade dos dados ou da exatidão; da limitação da conservação; da segurança, da integridade e da confidencialidade; da prestação de contas ou da responsabilização. E, para fins de melhor entendimento da discussão proposta, o princípio da minimização prevê que os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais serão processados, objetivando a redução do número de dados, de forma a serem coletados apenas aqueles que sejam essenciais.

O GDPR marcou tendência no mundo ao implementar medidas rígidas de proteção de dados, tratando-se de um sistema de governança que oferece aos cidadãos um conjunto de fortes direitos executórios necessários na garantia de uma maior privacidade e, consequentemente, da proteção de dados pessoais, sendo este considerado um direito fundamental (SARLET, 2020), derivado da fenomenologia da era digital, notadamente em decorrência das atividades crescentes de coleta, de processamento e de armazenamento daqueles dados. No entanto, deve-se enfatizar não haver que se falar em caráter absoluto desses direitos, visto a possibilidade de limitação quando houver colisão com direitos congêneres, o que demanda análise com sopesamento dos princípios.

5 O ESTADO INFORMACIONAL E A AUTODETERMINAÇÃO INFORMATIVA

Inegável que o direito à proteção da vida privada representou a concepção na solução do caso posto em discussão, eis que certa a repercussão na esfera íntima daqueles que foram afetados por meio do processamento de seus dados, o que justifica o fato dos direitos

fundamentais serem reconhecidos como princípios norteadores no desenvolvimento de uma legislação direcionada à proteção de dados, demonstrando, em grande medida, não existirem dados irrelevantes para fins de processamento eletrônico, assim como o fato dos direitos fundamentais terem importância na proteção em face das violações e ingerências estatais, o que perpassa pela análise do direito à autodeterminação informacional, derivada do julgamento realizado pelo Tribunal Constitucional Federal da Alemanha na decisão sobre o censo populacional em 1983.

Nesse sentido, ao abordar a questão do Estado informacional, Braman (2006) destaca no livro *Change of State,* a desproporcionalidade da relação informacional do Estado para com os cidadãos, na medida em que aquele, munido de novas tecnologias da informação e da comunicação (TIC) e, por meio das diversas interfaces digitais, possui capacidade de alcançar qualquer pessoa com acesso à internet, sendo indicado três fatores que sustentam essa afirmação: (i) os mecanismos de vigilância são de via única – os cidadãos são monitorados e nem sequer têm a noção de estarem sendo observados; (ii) os cidadãos perderam a capacidade de escolher, determinar, filtrar ou selecionar quais de suas informações estarão disponíveis para a consulta pública; (iii) as informações deliberadamente selecionadas e disponibilizadas por terceiros funcionam como subsídios de sustentação do regime de vigilância total.

Assim, diverso do sistema de vigilância exercido pelo Estado burocrático indicado por Jeremy Bentham no dispositivo panóptico[24], referente a um projeto arquitetônico de um complexo penitenciário que se tornou o ícone do estado utilitarista, por permitir a um único vigilante observar todos os prisioneiros, sem que estes saibam que estão sendo observados, levando-os a adotar um comportamento desejado pelo vigilante, o qual foi posteriormente recuperado por Foucault (2012), para indicar um modelo de vigilância centralizado que se limitava a indivíduos inseridos em um determinado ambiente, denominado de "sociedade disciplinar", vislumbra-se no Estado informacional, o modelo *panspectron,* utilizado em primeira mão no livro de Manuel DeLanda (1991, p. 206), posteriormente indicado por Branden Hookway (2000), que representa a implantação de um sistema de vigilância ampliada de todos os corpos, em escala continental e ubíqua, pelo processamento de filtros ou de listas de observação de palavras-chave e, dessa maneira, da compilação das informações de forma abrangente, indireta e constante, no qual o alvo da vigilância é conhecido com base em padrões e identificado por um processo de lógica inferencial aplicado a grande quantidade de dados.

[24] Conquanto não tenha sido projetado, o modelo foi utilizado como base para a arquitetura de alguns complexos prisionais, tais como: Milbank e Pentonville em Londres (respectivamente, 1812-1902 e 1842), Stateville em Illinous (USA – 1295) e o Presídio Modelo na Ilha da Juventude em Cuba (1925-1973).

As novas ferramentas tecnológicas de informação e comunicação (nTIC) propiciam analisar os padrões comportamentais gerados pelo próprio usuário que assume um papel coadjuvante ao fornecer os mais diversos dados que podem vir estruturados inclusive dos dispositivos digitais (metadados), auxiliando, com isso, na sua descrição e identificação, fazendo com que conceitos como privacidade e individualidade sejam postos à margem, mormente se considerada a exponencial assimetria informacional existente entre Estado e cidadão que, sob a justificativa de interesses públicos, tal como analisado no caso do sistema de vigilância de dados que utiliza o modelo de risco algorítmico oculto, demonstra a dificuldade em se estabelecer uma relação harmônica entre Estado, vigilância e democracia, já que direitos como liberdade, intimidade e informação apresentam-se vulneráveis diante do poder daquele regime de vigilância de massa.

A questão, então, demanda um maior e mais amplo reconhecimento da autodeterminação informativa, como forma de garantir aos cidadãos o direito de saber como e para qual finalidade seriam utilizados seus dados e, com isso, decidir em que medida poderia ter suas informações publicadas ou processadas, sob pena de afronta ao direito fundamental da privacidade e da proteção de dados, cuja tutela tem se revelado cada vez mais difícil diante das "crescentes oportunidades oferecidas pela sociedade da informação", já que a pessoa se vê "obrigada a expor seu próprio eu, em sua própria persona", fazendo com que os dados fornecidos à sua revelia passem a ser uma "espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito" (RODOTÁ, 2008, p. 113).

Nesse contexto, diante do avanço das tecnologias da informação, ressalte-se a essencialidade e a indispensabilidade da existência de regras sólidas, como forma de compelir o Estado a intervir, por meio de órgãos fiscalizadores, para fins de efetivar o direito à autodeterminação informativa e, assim, possibilitar que o cidadão seja efetivamente informado quanto ao objetivo da coleta, do processamento e do armazenamento de seus dados por terceiros ou qualquer entidade e, mediante tal conhecimento, ter a liberdade de escolher as ações que poderão ser ou não realizadas, com vistas à proteção e ao controle do uso de suas informações pessoais, de modo a denotar o respeito adequado aqueles direitos e alcançar o ideário de uma sociedade democrática apropriada ao cenário atual.

6 CONCLUSÃO

As numerosas oportunidades proporcionadas pelas transformações digitais vêm acompanhadas de grandes desafios, mormente no que se refere à proteção de dados, ante a vulnerabilidade em relação a ferramentas digitais que possibilitam a ocorrência de vigilâncias

intrusivas, usurpação de identidade, discriminação de pessoas, preconceitos sistemáticos, dentre outras, que dificultam o estabelecimento de uma relação harmônica entre Estado, vigilância e democracia.

O reconhecimento do direito à proteção de dados vem se convertendo em um fenômeno de convergência mundial como um direito central, deixando de ser apenas um direito fundamental da pessoa e passando a ser, também, uma questão de interesse público, que deve ser considerado à luz de sua função social, tal como ressalta o artigo 4º do GDPR, para, ao fim e ao cabo, salvaguardar a justa finalidade no processamento de dados pessoais e o direito à autodeterminação informativa, sendo este a pedra de toque, na medida em que deve possuir um alcance maior em comparação à compreensão clássica do direito à privacidade, pois, tratando-se de um direito ainda recente e de caráter relevante, consequentemente, possibilita uma maior amplitude na tomada de decisão do indivíduo no contexto da aceitação na divulgação, processamento e uso daqueles dados contra qualquer violação e ingerência.

Deve-se apontar, nessa altura, que em razão dos agravos advindos das condutas de gigantes tecnológicos de natureza transnacional, trata-se de um direito que alcança um âmbito de proteção típico dos direitos humanos, ou seja, indo além da atuação dos Estados.

Justifica-se, de qualquer sorte, a importância de regulamentação legal que estabeleça exigências constitucionais de proteção dos dados como padrão central dos direitos fundamentais, levando em conta as exigências dos princípios da clareza, da finalidade, da minimização, da determinação e da proporcionalidade no processamento.

A decisão que fora analisada, envolvendo o governo holandês e o sistema de indicação de risco, jogou luzes sobre os impactos que a implantação de uma ferramenta de vigilância informacional - com análise preditiva e sem transparência quanto ao tratamento de dados na indicação de perfil - ser capaz de ocasionar, porquanto traduzir o desrespeito ao direito à privacidade das pessoas, à proteção de dados pessoais, assim como levar a um possível efeito estigmatizante e discriminatório, o que reforça a obrigatoriedade no repasse de informação aos titulares quanto ao uso, conservação e tratamento dos dados fornecidos, a adoção de medidas técnicas e organizativas de segurança do tratamento das informações, bem ainda a necessária proteção dos dados desde a fase inicial da coleta. E, sobretudo, evoca a urgência de um amplo debate sobre o papel dos Estados e das empresas privadas nesse panorama que, por vezes, se mostra hermético para o cidadão comum.

Tais considerações demonstram a importância da proteção da pessoa humana, a qual deverá estar sempre na posição central da ordem jurídica, motivo pelo qual a conscientização

cada vez maior dos cidadãos sobre o intenso fluxo de informações pessoais possibilita maior consciência e, de certo modo, oportunizam o acautelamento no fornecimento de seus dados.

O movimento de vigilantismo na atual arena de poder eminentemente globalizada e permeada pelas TICs tem sido frequentemente utilizado sem que as suas consequências sejam levadas a público a sério, independentemente do volume e da densidade dos danos às pessoas e aos usuários direta e indiretamente afetados. Urge reafirmar que tal situação deve ser alvo de uma intensa discussão pela sociedade civil para que, com isto, se possa emular novas pautas para a solução de conflitos e, assim, reforçar a eficácia do catálogo de direitos que podem e devem ser as balizas que asseguram as condições de exercício da cidadania digital.

REFERÊNCIAS

ALBERS, Marion. **A complexidade da proteção de dados**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 10, n. 35, p. 19-45, jul./dez. 2016. Disponível em: file:///C:/Users/notebookFA/Documents/Doutorado/Ingo%20Sarlet_Dir.%20Fundamentais%20na%20Sociedade%20Tecnológica%20e%20da%20Informação/ALbers%20A%20complexidade%20da%20proteção%20de%20dados%20DFJ%20artigo.pdf. Acesso em: 11 jun. 2020.

BENTHAM, Jeremy. ***Panopticon***: postscript; part I – containing further particulars and alterations relative to the plan of construction originally proposed; principally adapted to the purpose of a panopticon penitentiary-house. London: T. Payne, 1791.

BRAMAN, Sandra. ***Information policy and power in the information State***. In: _____. Change of State. Cambridge, MA: MIT Press, 2006. cap. 9, p. 313-328.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018 (**Lei Geral de Proteção de Dados Pessoais)**. Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2020.

BRUNO, Fernanda. **Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas.** Revista Fronteiras – estudos midiáticos. VIII, Nº 2: p. 152-159, maio/agosto 2006. Disponível em: file:///C:/Users/notebookFA/Downloads/6129-18735-1-SM.pdf. Acesso em 31 ago. 2020.

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2016/C 202/02). **Jornal Oficial da União Europeia**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR). PDF. Acesso em 12 maio 2020.

CIANCONI, Regina de Barros; LOTT, Yuri Monnerat. **Do panopticon ao panspectron**: uma reflexão sobre as mediações de poder e a materialidade da informação. Liinc em Revista, Rio de Janeiro, v.12, n.2, p. 243-257, novembro 2016; Disponível em: file:///C:/Users/notebookFA/OneDrive/Documentos/Doutorado/Ingo%20Sarlet_Dir.%20Fundamentais%20na%20Sociedade%20Tecnológica%20e%20da%20Informação/Pansprecton_Vigilância%20informacional.pdf. Acesso em 11 jun. 2020.

COLOMBO, Cristiano; NETO, Eugênio Facchini. **Mineração de dados e análise preditiva**: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. Rev. de Direito, Governança e Novas Tecnologias. e-ISSN: 2526-0049. Maranhão. v. 3, n. 2, p. 59–80. Jul/Dez. 2017. Disponível em: file:///C:/Users/notebookFA/Downloads/2345-11271-1-PB%20(2).pdf. Acesso em: 11 jun. 2020.

COMISSÃO EUROPEIA. **Comunicação da Comissão ao Parlamento Europeu e ao Conselho:** As regras de proteção de dados como instrumento gerador de confiança dentro e fora da EU – ponto da situação. Bruxelas, 24.7.2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019DC0374&from=EN). PDF. Acesso em 12 maio 2020.

DELANDA, M. ***War in the age of intelligent machines***. New York: Zone Books, 1991. Disponível em: https://www.scielo.br/scielo.php?script=sci_nlinks&pid=S1413-99362017000400068000009&lng=. Acesso em: 11 jun. 2020.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. 2ª edição. São Paulo: Revista dos Tribunais, 2019.

FOUCAULT, M. **Vigiar e punir**: nascimento da prisão. Petrópolis: Vozes, 2012. (Disponível em: https://www.scielo.br/scielo.php?script=sci_nlinks&pid=S1413-99362017000400068000012&lng=en Acesso em: 15 maio 2020.

HOFFMANN-RIEM, Wolfang. Inteligência artificial como oportunidade de regulação jurídica. *Revista de Direito Público*, nº 90, volume 16, nov.-dez., p. 11-38, 2019.

INSIDE China´s Vast New Experiment in Social Ranking. Wired. 14 dezembro 2017. Business. Disponível em: https://www.wired.com/story/age-of-social-credit/. Acesso em: 1º set. 2020.

INTERNETLAB Pesquisa em direito e tecnologia. [Holanda] **Tribunal decide que Sistema de Indicação de Risco viola direitos humanos**. 11 fev. 2020. *Blog.* Disponível em: https://www.internetlab.org.br/pt/itens-semanario/holanda-tribunal-decide-que-sistema-de-indicacao-de-risco-viola-direitos-humanos/. Acesso em: 12 maio 2020.

KANASHIRO, M. M.; BRUNO, F. G.; EVANGELISTA, R. A.; FIRMINO, R. J. Big data: reconstrução e disputa por novos significados de privacidade. **Portal das Ciências Sociais Brasileiras**, [*s. l.*], ano 37º Anual da ANPOCS, 9 out. 2013. Disponível em: http://www.anpocs.com/index.php/encontros/papers/37-encontro-anual-da-anpocs/st/st27/8783-big-data-reconstrucao-e-disputa-por-novos-significados-de-privacidade. Acesso em: 1 set. 2020.

MARQUESONE, Rosangela. **Big data**: técnicas e tecnologias para a extração de valor de dados. São Paulo: Casa do Código, 2016.

MENDES, Laura Schertel. ***Privacidade, proteção de dados e defesa do consumidor****: Linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014.

_____ Laura Schertel; MATTIUZZO, M. **Discriminação Algorítmica**: Conceito, Fundamento Legal e Tipologia. *Revista Direito Público*, v. 16, 2019.

_____ Laura Schertel Ferreira. **Habeas data e autodeterminação informativa**: os dois lados da mesma moeda. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. Disponível em: file:///C:/Users/notebookFA/Documents/Doutorado/Ingo%20Sarlet_Dir.%20Fundamentais%20na%20Sociedade%20Tecnológica%20e%20da%20Informação/artigo%20Laura%20Mendes%20Habeas%20data%20e%20autodeterminaçao%20informativa%20RDFJ%202018.pdf. Acesso em 13 maio 2020.

NEOTEL Segurança Digital. **Primeira decisão europeia que declara ilegal um algoritmo para avaliação das características pessoais dos titulares de dados**. 17 fev. 2020. *Blog*. Disponível em: https://www.neotel.com.br/blog/2020/02/17/primeira-decisao-europeia-que-declara-ilegal-um-algoritmo-para-a-avaliacao-das-caracteristicas-pessoais-dos-titulares-de-dados/. Acesso em: 12 maio 2020.

NETHERLANDS. Rechtbank Den Haag. Zaaknummer: **C-09-550982-HA ZA 18-388**. SYRI-WETGEVING in strijd met het Europees Verdrag voor de Rechten voor de Mens. ECLI: NL: RBDHA: 2020: 865. Rechtbank Den Haag, 5 fev. 2020. Disponível em: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865. Acesso em: 12 maio 2020.

NETHERLANDS. **Wet Structuur Uitvoeringsorganisatie Werk en Inkomen**. Structure of the organisation of the implementation of the Labour and Income Act. [2001]. Disponível: https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=68942&p_lang=. Acesso em: 12 maio 2020.

NETHERLANDS. **Besluit SUWI**, de 20 de dezembro de 2001. [Adota uma ordem no conselho para implementação da Lei de Trabalho e Renda – Organização de Implementação – em conexão com outras leis de previdência social. Overheil.nl.
Disponível em: https://wetten.overheid.nl/BWBR0013267/2020-01-01/#Hoofdstuk5_Paragraaf5.6_Artikel5.23. Acesso em 12 maio 2020.

ONU – **Carta das Nações Unidas de 1970.** São Francisco, Estados Unidos. Assinada em 26 de junho de 1945. Disponível em: https://nacoesunidas.org/wp-content/uploads/2017/11/A-Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf. Acesso em: 2 set. 2020.

PIOVESAN, Flávia; GOTTI, Alessandra Passos; MARTINS, Janaína Senne. **A Proteção Internacional dos Direitos Econômicos, Sociais e Culturais**. In PIOVESAN, Flávia (org.) Temas de Direitos Humanos. 4ª ed. São Paulo: Saraiva, 2010, p. 122

RIOS, Roger Raupp; LEIVAS, Paulo Gilberto Cogo; SCHÄFER, Gilberto. DIREITO DA ANTIDISCRIMINAÇÃO E DIREITOS DE MINORIAS: PERSPECTIVAS E MODELOS DE PROTEÇÃO INDIVIDUAL E COLETIVO. **Revista Direitos Fundamentais & Democracia**, [*S. l.*], ano 2017, v. 22, n. 1, p. 126-148, 30 abr. 2017. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/issue/view/v.%2022%2C%20n.%201%20%282017%29%3A%20Revista%20Direitos%20Fundamentais%20%26%20Democracia. Acesso em: 31 ago. 2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância** (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008, p. 113.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 13, n. 41, p. 183-212, jul./dez. 2019. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/811/964. Acesso em 11 jun. 2020.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica.com**. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em:http://civilista.com/o-consentimento-informado-e-a-protecao/. Data de acesso: 31 ago. 2020.

SARLET, Ingo Wolfgang. NETO, Arthur M. Ferreira. **O direito ao "esquecimento" na sociedade da informação.** Porto Alegre: Livraria do Advogado, 2019.

_____. (2020). PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA CONSTITUIÇÃO BRASILEIRA DE 1988. **Revista Brasileira de Direitos Fundamentais & Justiça**, 14(42), 179-218. Disponível em: https://doi.org/10.30899/dfj.v14i42.875. Acesso em: 3 set. 2020.

_____. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13ª ed. rev. e atual. - Porto Alegre: Livraria do Advogado, 2018.

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

STATE v. Loomis: Wisconsin Supreme Court Requires Warning Before Use Of Algorithmic Risk Assesments in Sentencing. **HARVARD LAW REVIEW**, [*s. l.*], 10 mar. 2017. Disponível em: https://harvardlawreview.org/2017/03/state-v-loomis/#:~:text=Loomis%20filed%20a%20motion%20for,Loomis%2C%20881%20N.W.&text=Loomis%20also%20argued%20that%20the,for%20the%20read%2Din%20charges. Acesso em: 2 set. 2020

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. [relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE]. **Jornal Oficial da União Europeia**. L 119/1. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679&cookies=disabled. Acesso em 12 maio 2020.