IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA)

DIREITO CIBERNÉTICO, LIBERDADE DE EXPRESSÃO E PROTEÇÃO DE DADOS II

D598
Direito cibernético, liberdade de expressão e proteção de dados II [Recurso eletrônico on-line] organização IV Congresso Internacional de Direito e Inteligência Artificial (IV CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Aghisan Xavier Ferreira Pinto, Marina de Castro Firmo e Luiza Santos Cury Soares – Belo Horizonte: Skema Business School, 2023.

Inclui bibliografia
ISBN: 978-65-5648-777-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os direitos dos novos negócios e a sustentabilidade.
1. Direito. 2. Inteligência artificial. 3. Tecnologia. I. IV Congresso Internacional de Direito e Inteligência Artificial (1:2023 : Belo Horizonte, MG).

CDU: 34

IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA)

DIREITO CIBERNÉTICO, LIBERDADE DE EXPRESSÃO E PROTEÇÃO DE DADOS II

Apresentação

O IV Congresso Internacional de Direito e Inteligência Artificial - CIDIA da SKEMA Business School Brasil, realizado nos dias 01 e 02 de junho de 2023 em formato híbrido, consolida-se como o maior evento científico de Direito e Tecnologia do Brasil. Estabeleceram-se recordes impressionantes, com duzentas e sessenta pesquisas elaboradas por trezentos e trinta e sete pesquisadores. Dezenove Estados brasileiros, além do Distrito Federal, estiveram representados, incluindo Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Pará, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Roraima, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos trinta e três grupos de trabalho do evento, que geraram uma coletânea de vinte e cinco livros apresentados à comunidade científica nacional e internacional, contou com a valiosa colaboração de sessenta e três professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo de double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre a relação entre inteligência artificial, tecnologia e temas como acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, sustentabilidade, democracia e responsabilidade civil, entre outros temas relevantes.

Um sucesso desse porte não seria possível sem o apoio institucional de entidades como o CONPEDI - Conselho Nacional de Pesquisa e Pós-graduação em Direito; o Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais; o Instituto Brasileiro de Estudos de Responsabilidade Civil - IBERC; a Comissão de Inteligência Artificial no Direito da Ordem dos Advogados do Brasil - Seção Minas Gerais; a Faculdade de Direito de Franca - Grupo de Pesquisa Políticas Públicas e Internet; a Universidade Federal Rural do Semi-Árido - UFERSA - Programa de Pós-graduação em Direito - Laboratório de Métodos Quantitativos em Direito; o Centro Universitário Santa Rita - UNIFASAR; e o Programa de Pós-Graduação em Prestação Jurisdicional e Direitos Humanos (PPGPJDH) - Universidade Federal do Tocantins (UFT) em parceria com a Escola Superior da Magistratura Tocantinense (ESMAT).

Painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional e internacional. A abertura foi realizada pelo Professor Dierle Nunes, que discorreu sobre o tema "Virada tecnológica no Direito: alguns impactos da inteligência artificial na compreensão e mudança no sistema jurídico". Os Professores Caio Lara e José Faleiros Júnior conduziram o debate. No encerramento do primeiro dia, o painel "Direito e tecnologias da sustentabilidade e da prevenção de desastres" teve como expositor o Deputado Federal Pedro Doshikazu Pianchão Aihara e como debatedora a Professora Maraluce Maria Custódio. Para encerrar o evento, o painel "Perspectivas jurídicas da Inteligência Artificial" contou com a participação dos Professores Mafalda Miranda Barbosa (Responsabilidade pela IA: modelos de solução) e José Luiz de Moura Faleiros Júnior ("Accountability" e sistemas de inteligência artificial).

Assim, a coletânea que agora é tornada pública possui um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da CAPES. Além disso, busca-se formar novos pesquisadores na área interdisciplinar entre o Direito e os diversos campos da tecnologia, especialmente o da ciência da informação, considerando a participação expressiva de estudantes de graduação nas atividades, com papel protagonista.

A SKEMA Business School é uma entidade francesa sem fins lucrativos, com uma estrutura multicampi em cinco países de diferentes continentes (França, EUA, China, Brasil e África do Sul) e três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua dedicação à pesquisa de excelência no campo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital requer uma abordagem transdisciplinar.

Expressamos nossos agradecimentos a todas as pesquisadoras e pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 14 de julho de 2023.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Caio Augusto Souza Lara

Coordenador de Pesquisa – SKEMA Law School for Business

COOKIES, PERFILIZAÇÃO E DISCRIMINAÇÃO ALGORÍTMICA

COOKIES, PROFILING AND ALGORITHMIC DISCRIMINATION

Marcos Vinícius Palomo Pessin [1]
José Luiz de Moura Faleiros Júnior [2]

Resumo

O processo de perfilização ('profiling') consiste na coleta de dados de titulares para criação de perfis comportamentais e oferece riscos à proteção de dados pessoais. A Lei Geral de Proteção de Dados Pessoais prevê em seu artigo 12, §2º, que os dados utilizados para formação do perfil comportamental de uma pessoa podem ser considerados dados pessoais para fins da lei, o que pode se dar a partir dos 'cookies'. No entanto, a ausência de instrumentos específicos para prevenção desses riscos acarreta problemas, pois até mesmo técnicas menos invasivas podem gerar discriminação. Portanto, defende-se a regulação específica para algoritmos de perfilização.

Palavras-chave: Cookies, Perfilização, Discriminação algorítmica, Proteção de dados pessoais

Abstract/Resumen/Résumé

The process of profiling involves collecting data from data subjects to create behavioral profiles, and poses risks to the protection of personal data. The Brazilian General Data Protection Law states in article 12, §2 that data used to create a behavioral profile can also be considered personal data under the law, which can be gathered through cookies. However, the absence of specific tools to prevent these risks can result in problems, as even less invasive techniques can lead to discrimination. Therefore, this summary argues for the need for specific regulation of profiling algorithms to prevent these risks.

Keywords/Palabras-claves/Mots-clés: Cookies, Profiling, Algorithmic discrimination, Personal data protection

[1] Pós-graduado em Direito Digital pela UERJ/ITS. Bacharel em Direito pela USP. Advogado.

[2] Doutorando em Direito pela USP e pela UFMG. Mestre e Bacharel em Direito pela UFU. Advogado e Professor. Orientador.

1. Introdução

A coleta de dados sobre a atividade online de usuários de *sites*, geralmente com fins publicitários para segmentação de anúncios, depende do uso de *cookies*. A partir desses dados, é possível prever os interesses e preferências desses usuários, formando um conjunto de informações que é operacionalizado por algoritmos para fornecer um perfil comportamental, processo conhecido como *profiling*.

Embora o *profiling* seja uma ferramenta importante para as empresas responsáveis por *sites*, ele oferece riscos de violação à proteção dos dados pessoais de seus usuários, uma vez que a construção de um perfil pessoal pode identificá-los, atraindo a aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou "LGPD"). Devido a esses riscos, ainda que de forma tímida, o legislador previu no art. 12, §2º, da LGPD, que "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".

Apesar de existirem técnicas de *profiling* menos invasivas que não exigem a identificação dos usuários, como a segmentação com base em características demográficas, essas técnicas também podem resultar em riscos, como discriminação em situações em que os usuários de um determinado grupo são tratados de forma diferente pelo algoritmo.

Nesse contexto, surge o tema-problema deste resumo: considerando a coleta de dados por meio de *cookies,* os instrumentos previstos na LGPD são suficientes para a prevenção de riscos envolvendo *profiling*? Este resumo defenderá a necessidade de uma regulação específica para algoritmos de perfilização devido à ausência de instrumentos na LGPD para a prevenção desses riscos.

A pesquisa será conduzida pelo método dedutivo, com uma breve revisão conceitual e exploração de uma possível conclusão para o tema-problema a partir da combinação da norma citada. A abordagem qualitativa será realizada, com aportes doutrinários que corroboram a defesa pretendida.

2. O que são *cookies* e como são utilizados para *profiling* na internet?

O conceito de *cookies* surgiu na década de 1990, quando empresas começaram a desenvolver a primeira geração de *sites* e a internet começou a se popularizar. Naquela época, era complexo para os *sites* rastrearem os usuários e suas preferências de navegação, o que tornava difícil fornecer uma experiência personalizada.

Os primeiros *cookies* eram pequenos arquivos de texto armazenados no computador do usuário pelo servidor do site que visitava. Esses arquivos continham informações básicas, como as preferências de idioma e as configurações de exibição, que ajudavam a personalizar a experiência do usuário. Os *cookies* funcionam da seguinte maneira: o usuário acessa um *site* usando um navegador web; o *site* envia uma pequena quantidade de dados para o navegador do usuário na forma de um *cookie*; o navegador armazena o *cookie* em um arquivo no computador do usuário; quando o usuário retorna ao *site*, o navegador envia o *cookie* de volta para o site para permitir que ele reconheça o usuário e personalize a experiência de navegação.

Embora comumente conhecidos por esse nome, os *cookies* são bastante diversificados e possuem classificações relevantes para sua compreensão. Em relação à sua duração no dispositivo do usuário, podem ser de sessão ou permanentes. Os primeiros não possuem data de validade e são automaticamente excluídos quando o navegador é fechado, enquanto os permanentes possuem prazo de validade e podem durar horas, dias, meses ou até anos (Koch, 2019).

A depender da necessidade, os *cookies* podem ser classificados como necessários ou opcionais, sendo os necessários essenciais para o funcionamento do site, e os opcionais utilizados para outras finalidades, como performance, funcionalidades e publicidade (Koch, 2019). Exceto quando as informações coletadas são anonimizadas, como pode ocorrer com *cookies* de performance, os *cookies* são considerados dados pessoais e estão sujeitos à LGPD.

Os *cookies* também são classificados como primários (*first-party cookies*) ou de terceiros (*third-party cookies*), sendo os primeiros de responsabilidade do site que o usuário está acessando e os de terceiros de responsabilidade de *sites* diferentes do acessado pelo usuário, como redes sociais (Koch, 2019).

À medida que a tecnologia evoluiu, os *cookies* se tornaram mais sofisticados e capazes de coletar informações mais detalhadas sobre o usuário, como seu histórico de navegação, localização geográfica e até mesmo seu tempo de permanência em determinada página, chegando ao ponto de catalogarem, em plataformas de redes sociais, as famigeradas reações (*likes*, *dislikes* etc.). Isso permitiu que as empresas criassem perfis detalhados de usuários, o que, por sua vez, permitiu que elas fornecessem experiências altamente personalizadas e segmentadas. No entanto, o uso de *cookies* também se tornou controverso devido a preocupações com a privacidade e a segurança dos dados pessoais dos usuários. Os *cookies* persistentes podem rastrear a atividade do usuário em vários *sites* ao longo do tempo, o que pode ser visto como uma invasão de privacidade.

Os *cookies* de terceiros, por sua vez, são considerados invasivos, pois não são enviados pelo site acessado pelo usuário, mas por terceiros associados ao site, geralmente fora da expectativa dos usuários. Além disso, os *cookies* também podem ser usados para coletar informações sensíveis sem o conhecimento do usuário. Por isso, no Brasil, é importante que as empresas responsáveis por *sites* adotem práticas transparentes e éticas em relação ao uso de *cookies* para garantir a privacidade e segurança dos dados dos usuários.

Nesse sentido, destaca-se o Guia Orientativo da Autoridade Nacional de Proteção de Dados (ANPD) sobre "*Cookies* e Proteção de Dados". O guia não apenas sugere formas de garantir a conformidade com a LGPD, mas também aborda suas bases legais que justificam o tratamento de dados pessoais. Ele se concentra em como as bases do consentimento e do interesse legítimo se aplicam às diversas categorias de *cookies* mais usadas em *sites*. Além disso, o documento apresenta exemplos de boas práticas que os controladores podem adotar para criar políticas e *banner*s de *cookies* mais apropriados.

Em relação ao *profiling*, a própria ANPD destaca nesse guia: "Os riscos à privacidade podem ser ampliados nas situações em que a falta de transparência está associada a práticas de coleta de quantidades massivas de informações pessoais para fins de identificar, rastrear e criar perfis comportamentais de usuários".

Desse modo, a associação de *cookies* e *profiling* eleva o risco das atividades de tratamento de dados pessoais relacionadas, o que merece especial atenção das empresas para mitigar esses riscos, em especial no que se refere à transparência e adoção da base legal adequada.

3. A perfilização a partir de decisões automatizadas: a gestão algorítmica de perfis

A promulgação da LGPD trouxe à tona um dos assuntos mais inquietantes concernentes à prática denominada *profiling* (ou 'perfilização', como a doutrina convencionou chamar). Como foi dito na introdução, um dispositivo bastante tímido, inserido em um único parágrafo do artigo que cuida da anonimização de dados na LGPD (art. 12, §2º), conceitua a referida prática.

A doutrina já se dedica há tempos à compreensão dos desdobramentos jurídicos da perfilização, antevendo os principais impactos da discriminação algorítmica. Nesse contexto, são expressivos os registros de William Staples (2007, p. 93) quanto à violação que isso causa ao direito fundamental à privacidade, e também o são as preocupações elencadas por Michael

Froomkin (2000, p. 1465) acerca da necessidade de que sejam adotadas contramedidas urgentes a tais práticas, sob pena de se passar a viver sem qualquer privacidade.

Existem diversas plataformas que utilizam *cookies* para realizar o *profiling* de usuários. Algumas das mais conhecidas incluem: (i) Google, que utiliza *cookies* para coletar informações sobre a atividade do usuário em seus vários serviços, como o Google Search, Google Maps e YouTube, com intenção de personalizar anúncios e recomendações de conteúdo com base nos interesses do usuário; (ii) Facebook, que utiliza *cookies* para rastrear a atividade do usuário na rede social e em *sites* de terceiros que utilizam o Facebook Pixel, uma ferramenta de análise de dados que permite que o Facebook crie perfis detalhados de usuários com base em seus interesses, comportamentos de compra e outras informações; (iii) Amazon, que utiliza *cookies* para rastrear a atividade do usuário em seu site e em *sites* de terceiros que fazem parte do programa de publicidade da Amazon, o que permite que a empresa personalize recomendações de produtos com base nas preferências do usuário.

Essas plataformas utilizam *cookies* de sessão, que são armazenados apenas temporariamente no navegador do usuário durante uma sessão de navegação, e *cookies* persistentes, que são armazenados no navegador por um período mais longo. Além disso, podem utilizar outras técnicas de rastreamento, como o armazenamento local de dados e a utilização de *tags* de conversão para coletar informações sobre a atividade do usuário em *sites* de terceiros. Tudo isso contribui para a criação de perfis detalhados de usuários com base em seus comportamentos e preferências online.

Uma das principais preocupações com a prática de *profiling* é a possibilidade de discriminação algorítmica. Isso acontece quando o perfil criado a partir do comportamento online do usuário é utilizado para tomar decisões automatizadas que podem afetar sua vida, como oferta de serviços, concessão de crédito ou mesmo decisões de emprego, gerando situações de exclusão e desigualdade, com potencial de violação do princípio da não discriminação da LGPD (art. 6º, IX).

Outro ponto relevante é a necessidade de uma base legal para o tratamento de dados de usuários de *sites* para fins de *profiling*. Em conformidade com o entendimento da ANPD no referido guia sobre *cookies*, entende-se que para essa finalidade as bases legais sejam o consentimento ou o legítimo interesse, sendo dever da empresa controladora dos dados observar os requisitos da LGPD e adotar a base legal que mais compatível com suas práticas de *profiling*.

Ainda, a LGPD estabelece que as decisões automatizadas com potencial de afetar interesses individuais têm de ser transparentes e proporcionais, além de permitir o direito à

revisão por parte do titular dos dados. Esse direito, previsto no art. 20 da LGPD, permite que a pessoa com interesses afetados solicite a revisão de decisões tomadas, unicamente, de modo automatizado. O objetivo desse direito é garantir que o indivíduo possa questionar e, se necessário, contestar a decisão tomada, assegurando que não haja prejuízo a seus direitos fundamentais, especialmente em situações de potencial discriminação.

Por fim, outro instrumento previsto na LGPD para prevenir riscos relacionados a decisões automatizadas envolvendo dados pessoais consiste na possibilidade de auditoria pela ANPD, nos termos dos arts. 20, §2º, e 55-J, inc. XVI. A ANPD poderá realizar auditoria para verificar o cumprimento das normas de proteção de dados, incluindo a análise das medidas adotadas para garantir a transparência, a não-discriminação e a imparcialidade desses processos decisórios. Desse modo, apesar de representar um marco na proteção dos dados pessoais no Brasil, a LGPD apresenta limitações no que diz respeito ao *profiling*, tendo em vista que ela somente se aplica a dados pessoais, excluindo alguns perfis comportamentais do seu escopo.

4. Horizontes possíveis: a proteção de direitos a partir da consideração dos perfis como extensões da identidade

Em 2010, Serge Gutwirth e Mireille Hildebrandt (2010, p. 37) defenderam a necessidade de que a criação de perfis pressuponha um sistema de proteção contra o processamento de dados que afeta comportamentos, mesmo que esses dados não possam ser considerados dados pessoais (caso dos *cookies*, embora possam se sujeitar excepcionalmente à LGPD, pela exegese do artigo 12, §2º).

Sem um instrumento vigoroso como a LGPD para que se possa esperar legitimamente um 'uso ético' dos algoritmos (MITTELSTADT; ALLO; TADDEO et al, 2016, passim), grande nebulosidade continuará a pairar sobre os processos utilizados para o monitoramento de comportamentos em redes sociais e as bases fundamentais para a definição de tão importante marco protetivo – com destaque para os direitos fundamentais à privacidade, à liberdade e à intimidade (art. 17, LGPD) – permanecerão no vazio em razão da própria dificuldade de se desvendar abusos e excessos praticados nos processos de tratamento de dados.

Além disso, é importante ressaltar que a proteção da identidade dos indivíduos não deve se limitar apenas ao âmbito dos dados pessoais, mas deve se estender a outros elementos que possam compor a sua identidade, como os perfis comportamentais. Nesse sentido, a privacidade ser vista como um meio para garantir a proteção dos direitos fundamentais,

incluindo o direito à igualdade, à não discriminação e à dignidade humana, que podem ser comprometidos pela criação e uso de perfis comportamentais sem a devida proteção.

Portanto, é fundamental que sejam estabelecidos mecanismos de proteção e controle efetivos para garantir que o uso de perfis comportamentais não afete negativamente a privacidade, a liberdade e a dignidade dos indivíduos. A adoção de padrões éticos e transparentes para o uso de algoritmos de criação de perfis, bem como a regulação do tema no âmbito das iniciativas envolvendo inteligência artificial, são medidas importantes para assegurar uma proteção adequada dos direitos dos indivíduos em relação ao uso de perfis comportamentais.

5. Considerações finais

Ao longo deste artigo, discutimos a importância da proteção de dados pessoais e o papel dos perfis comportamentais nesse contexto. Vimos que a criação de perfis pode ser útil para personalizar experiências e melhorar serviços, mas também pode levar a riscos à privacidade e à liberdade individual, além de discriminação. Por isso, é essencial que haja instrumentos regulatórios efetivos, como a LGPD, para garantir que o tratamento de dados ocorra de maneira ética e respeitando os direitos fundamentais dos indivíduos.

Contudo, também apontamos para a limitação da LGPD em lidar com todos os riscos decorrentes do *profiling*, uma vez que ela só se aplica a dados pessoais e há esferas de privacidade além disso que podem ser violadas por perfis comportamentais que não permitem a identificação dos indivíduos. Nesse sentido, consideramos que a proteção de direitos deve ser ampliada a partir da consideração dos perfis como extensões da identidade, visando a garantir a preservação da privacidade, da liberdade e da intimidade em todas as esferas da vida.

Assim, destacamos a importância de se avançar na discussão sobre o tema e no desenvolvimento de novas soluções regulatórias para garantir uma proteção cada vez mais ampla e efetiva dos direitos fundamentais dos indivíduos diante dos riscos decorrentes do *profiling*.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo:** Cookies e proteção de dados pessoais. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf Acesso em: 29 abr. 2023.

DENSA, Roberta; DANTAS, Cecília. Notas sobre publicidade digital: *cookies* e *spams*. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). **Direito digital**: direito privado e internet. 4. ed. Indaiatuba: Foco, 2021. p. 689-704.

FROOMKIN, A. Michael. The death of privacy? **Stanford Law Review**, Stanford, v. 32, p. 1461-1544, maio 2000.

GUTWIRTH, Serge; HILDEBRANDT, Mireille. Some caveats on profiling. *In:* GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (ed.). **Data protection in a profiled world**. Cham: Springer, 2010. p. 31-42.

HILDEBRANDT, Mireille. Who is profiling who? Invisible visibility. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul *et al* (ed.). **Reinventing data protection?** Dordrecht: Springer, 2009. p. 239-252.

LYON, David. **The electronic eye**: the rise of surveillance society. Minneapolis: University of Minnesota Press, 1994.

LYON, David. Surveillance as social sorting: computer codes and mobile bodies. In: LYON, David (ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. Londres: Routledge, 2003. p. 13-30.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria *et al*. The ethics of algorithms: mapping the debate. **Big Data & Society**, Londres: Sage, Original Research Article, p. 1-21, jul./dez. 2016.

KOCH, Richie. **Cookies, the GDPR, and the ePrivacy Directive**. GDPR.EU. Disponível em: https://gdpr.eu/cookies/. Acesso em: 03.05.2023.

PESSIN, Marcos Vinícius Palomo. **Cookies e proteção de dados no Brasil**: hipóteses legais aplicáveis. 2022. 28 f. Trabalho de Conclusão de Curso (TCC), Universidade do Estado do Rio de Janeiro, Centro de Estudos e Pesquisas no Ensino do Direito (Ceped), Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), Rio de Janeiro, 2022.

STAPLES, William G. **Encyclopedia of privacy**. Westport: Greenwood Press, 2007.

VAN DER PLOEG, Irma. Biometrics and the body as information: normative issues of the socio-technical coding of the body. In: LYON, David (ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. Londres: Routledge, 2003. p. 57-74.

ZANATTA, Rafael. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados. **ResearchGate**. fev. 2019. Disponível em: https://bit.ly/3hQe5wM. Acesso em: 25 abr. 2023.

ZIMMERMAN, Rachel K. The way “cookies” crumble: Internet privacy and data protection in the Twenty-First Century. **NYU Journal on Legislation and Public Policy**, Nova York, v. 4, p. 439-464, 2000.