

A REGULAMENTAÇÃO DO USO DE DADOS POR PLATAFORMAS DIGITAIS: UMA ANÁLISE POR MIREILLE HILDEBRANDT.

Autor: Juliana Santolin de Lima

Orientador: Vinicius Fernandes Ormelesi

Grupo de Trabalho: Direito Digital e Economico (GT5)

INTRODUÇÃO: Mireille Hildebrandt é professora de direito na Universidade Livre de Bruxelas, também formada em Filosofia pela Universidade Erasmus de Roterdã, trabalha estudando a intersecção entre o direito e a tecnologia, analisando criticamente as consequências da relação e qual seus efeitos na constituição e aplicação Estado de Direito.

Em 2018 Mireille Hildebrandt ministrou uma aula no instituto de pesquisa científica The Alan Turing Institute, intitulada: "The Primitives of Legal Protection against Data Totalitarianisms: Professor Mireille Hildebrandt", onde abordou sobre o uso de dados pessoais (Cookies) por plataformas gratuitas como Facebook ou Google e como essa nova modalidade de comércio moldou o mercado digital. Além disso menciona pautas como o conceito de "Totalitarismo de Dados" (Data Totalitarianisms) diferenciando-o de "Tiranía de Dados" e sua relação direta com as consequências jurídicas que o uso não regulado de dados online pode provocar à vida privada.

Paralelamente a essas questões, no artigo intitulado "Data Protection by Design and Technology Neutral Law", Mireille Hildebrandt analisa o conceito de Data Protection by Design, posteriormente incorporado ao art. 25 do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR). A autora sustenta que a rápida evolução das tecnologias digitais impõe novos desafios à proteção dos direitos fundamentais, especialmente da privacidade e da proteção de dados pessoais. Nesse contexto, defende que a simples existência de normas jurídicas não é suficiente para assegurar a efetividade desses direitos, sendo necessário que a própria arquitetura dos sistemas tecnológicos seja concebida para incorporá-los desde a fase de desenvolvimento.

O presente trabalho busca analisar de que forma a teoria desenvolvida por Mireille Hildebrandt contribui para a compreensão da regulamentação do uso de dados pessoais por plataformas digitais gratuitas. Para tanto, investiga-se o conceito de Data Protection by Design previsto no GDPR e sua relevância como instrumento de proteção dos direitos fundamentais diante de modelos de negócio baseados na coleta, no tratamento e na exploração econômica de dados pessoais.

PROBLEMA DE PESQUISA: O Data Protection by Design constitui um mecanismo jurídico adequado para proteger os dados pessoais dos usuários de plataformas digitais gratuitas cujo modelo econômico depende da coleta e do tratamento de dados?

OBJETIVO: O presente trabalho busca analisar de que forma a teoria desenvolvida por Mireille Hildebrandt contribui para a compreensão da regulamentação do uso de dados pessoais por plataformas digitais gratuitas. Para tanto, investiga-se o conceito de Data Protection by Design previsto no GDPR e sua relevância como instrumento de proteção dos direitos fundamentais diante de modelos de negócio baseados na coleta, no tratamento e na exploração econômica de dados pessoais.

METODOLOGIA: O trabalho possui metodologia qualitativa exploratória bibliográfica, analisando os artigos de Mireille Hildebrandt, especialmente "Data Protection by Design and Technology Neutral Law (2013)" e, também, a aula ministrada pela autora no The Alan Turing Institute em 2018 intitulada "The Primitives of Legal Protection against Data Totalitarianisms: Professor Mireille Hildebrandt" disponível na plataforma YouTube.

DISCUSSÃO E RESULTADOS ALCANÇADOS: Durante a aula ministrada por Mireille Hildebrandt no The Alan Turing Institute, a professora de direito da Universidade Livre de Bruxelas, destaca como as plataformas online gratuitas reconfiguraram o mercado. Na era digital, foi "descoberto" o poder de dados como sendo mais útil e de maior interesse do mercado que de fato mensalidades e planos para ter acesso a determinado serviço, os dados pessoais de milhões de usuários vão muito além da simples recomendação de conteúdos e produtos específicos nas redes, podem ser usados para influenciar decisões e manipular opiniões.

Segundo Hildebrandt, ainda em sua palestra sobre proteção de dados, há no meio digital a possibilidade de "Totalitarismo de Dados". A autora difere totalitarismo da tirania, destacando que no modelo tirânico a vida privada ainda existe, já no totalitarismo o privado é completamente destruído, não sendo de direito alheio. Hildebrandt explica, em tradução livre:

Tirania significa que não existe uma esfera pública: a esfera pública é propriedade privada do príncipe, do rei ou do imperador. Já a esfera privada é, em certa medida, deixada em paz, porque, afinal, quem se importa? Por que o governante se preocuparia com o que você faz na sua vida privada? A vida pública é aquilo de que ele é proprietário. O totalitarismo vai mais fundo e mais longe. Ele significa a destruição da esfera privada: não se permite que ela exista de forma autônoma. Em vez disso, o Estado a invade e procura controlar e direcionar tudo o que acontece nela

Para unir as duas ideias apresentadas até aqui, o poder de empresas que armazenam dados (que não se resume a recomendação de produtos e propagandas de consumo) e o totalitarismo de dados, é possível traçar semelhanças ao escândalo envolvendo o Facebook e a Cambridge Analytica. Em 2014, o pesquisador Aleksandr Kogan desenvolveu um aplicativo de teste de personalidade denominado "*This Is Your Digital Life*", por meio do qual cerca de 270 mil usuários consentiram com o compartilhamento de seus dados. Entretanto, em razão das permis-

sões então concedidas pela API do Facebook, o aplicativo também coletou informações dos amigos desses usuários, sem que estes tivessem autorizado tal tratamento, resultando na obtenção de dados de aproximadamente 87 milhões de pessoas. Posteriormente, essas informações foram transferidas para a empresa Cambridge Analytica (Especializada em análise

de dados e estratégias de marketing político, a Cambridge Analytica colaborou com a campanha eleitoral de Donald Trump nas eleições presidenciais de 2016, nos Estados Unidos.), que as utilizou para elaborar perfis psicográficos dos usuários e direcionar campanhas políticas altamente personalizadas, especialmente durante a eleição presidencial norte-americana de 2016. O caso veio a público em 2018, após denúncias do ex-funcionário Christopher Wylie, revelando que os dados haviam sido utilizados para influenciar o comportamento eleitoral sem o conhecimento ou consentimento efetivo de seus titulares. As repercussões foram significativas: Mark Zuckerberg foi convocado a prestar esclarecimentos ao Congresso dos Estados Unidos, o Facebook foi multado em US\$ 5 bilhões pela Federal Trade Commission (FTC) por falhas na proteção da privacidade dos usuários, e a Cambridge Analytica encerrou suas atividades.

Aqui é possível notar a invasão direta de um setor privado, ao visar o lucro e a vantagem própria, na esfera privada de milhões de usuários, tendo estes concordado ou não com a coleta de seus dados. O que torna este caso ainda mais preocupante é a demonstração de como o armazenamento de dados é uma arma poderosa em tempos digitais, podendo ser usada, por exemplo, como no caso em análise, para influenciar decisões eleitorais.

Além das consequências jurídicas e econômicas, o episódio evidenciou as limitações do consentimento como único fundamento para o tratamento de dados pessoais e reforçou a necessidade de adoção de mecanismos preventivos de governança, transparência e responsabilidade, como a proteção de dados desde a concepção (*Data Protection by Design*).

Mireille Hildebrandt e Laura Tielemans (2013, p. 515 – 516) em seu artigo "Data Protection by Design and Technology Neutral Law", introduz a problemática que traz à tona a necessidade da aplicação de "*Data Protection by Design*":

Costuma-se afirmar que a rápida evolução tecnológica é prejudicada por legislações ultrapassadas. Pode ser que a simples tentativa de elaborar leis tecnologicamente neutras, capazes de permanecer válidas no futuro, seja uma causa perdida, corroendo tanto a força moral quanto a eficácia prática do Direito. Assim, a tentativa de elaborar uma legislação sustentável acaba produzindo insegurança jurídica, pois seus próprios comandos tornam-se insustentáveis diante de impactos tecnológicos que não poderiam ter sido previstos. Talvez a única forma de alcançar sustentabilidade nesse campo seja combinar normas gerais com a exigência de que, no nível do projeto técnico dos sistemas, as obrigações de proteção de dados sejam efetivamente incorporadas, sempre que isso for técnica e economicamente viável.

No capítulo seguinte Hildebrandt e Tielemans (2013, p. 516) introduz a ideia de proteção de dados desde sua concepção:

O Artigo 29 (Article 29 Working Party – Art. 29 WP) argumentou que o princípio da Proteção de Dados desde a Concepção (*Data Protection by Design*) deveria tornar-se uma obrigação jurídica, exigindo que a proteção tecnológica

dos dados fosse considerada desde a fase de planejamento dos Sistemas de Tratamento de Dados Pessoais (Personal Data Processing Systems – PDPSs). Essa abordagem pressupõe que a tecnologia é, de fato, aberta e capaz de incorporar valores e normas que vão além daqueles estritamente relacionados aos protocolos tecnológicos.

Aqui sustenta-se que a proteção de dados deveria deixar de ser apenas uma preocupação posterior ao desenvolvimento dos sistemas e passar a ser uma obrigação jurídica executada desde a fase de planejamento dos sistemas de tratamento de dados pessoais. Em outras palavras, a privacidade e a proteção dos dados não deveriam ser implementadas apenas depois que o software estivesse pronto, mas incorporadas desde sua concepção.

Cumpre observar que o artigo Data Protection by Design and Technology Neutral Law, publicado por Mireille Hildebrandt e Laura Tielemans em 2013, foi elaborado quando o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR) ainda se encontrava em fase de proposta legislativa. Assim, ao longo do texto, as autoras analisam criticamente a previsão do Data Protection by Design como uma futura obrigação jurídica. Posteriormente, com a aprovação, o instituto foi incorporado ao ordenamento jurídico europeu por meio do artigo 25, intitulado *Data Protection by Design and by Default*, tornando obrigatória a adoção de medidas técnicas e organizacionais destinadas a assegurar a proteção de dados pessoais desde a concepção e por padrão.

Mais adiante ao artigo a autora se compromete a explicar por que a implementação da proteção desde sua concepção é eficaz:

Em primeiro lugar, a obrigação de implementar o Data Protection by Design (DPbD) é dirigida aos controladores de dados. Isso significa que ela se destina aos usuários das tecnologias e técnicas de tratamento de dados, e não aos seus projetistas ou fabricantes. A ideia parece ser que, ao tornar os controladores responsáveis (e juridicamente responsabilizáveis), eles pressionarão os desenvolvedores a criarem tecnologias adequadas.

Hildebrandt parte da definição jurídica europeia de controller, que atualmente está no artigo 4(7) do GDPR:

Controlador" significa a pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outros, determina as finalidades e os meios do tratamento de dados pessoais. Quando as finalidades e os meios desse tratamento forem determinados pelo Direito da União Europeia ou pelo direito de um Estado-Membro, o controlador ou os critérios específicos para sua designação poderão ser estabelecidos pelo Direito da União ou pelo

direito do Estado-Membro.

Por último, Mireille e Laura (2013 p. 520) concluem:

Os autores sustentam que a obrigação de incorporar a proteção de dados desde a concepção concilia três objetivos fundamentais: **(i)** compensar os efeitos prejudiciais decorrentes do funcionamento dos sistemas de tratamento de dados pessoais; **(ii)** preservar condições equitativas de concorrência, estimulando a inovação e evitando vantagens competitivas injustificadas para tecnologias já existentes ou emergentes; e **(iii)** manter um grau de abstração normativa suficientemente amplo para garantir a sustentabilidade da regulação diante da constante evolução tecnológica.

Em síntese, o Data Protection by Design permite tornar a proteção de dados mais efetiva ao exigir que as garantias legais sejam incorporadas desde a concepção dos sistemas. Com isso, busca reduzir os riscos inerentes ao tratamento de dados pessoais, além de criar uma obrigação jurídica suficientemente ampla para permanecer aplicável mesmo diante das constantes transformações tecnológicas.

CONCLUSÃO: A análise da teoria desenvolvida por Mireille Hildebrandt permite concluir que a crescente exploração econômica dos dados pessoais por plataformas digitais gratuitas representa um dos maiores desafios contemporâneos à proteção dos direitos fundamentais. Conforme demonstrado pela autora, o tratamento massivo de informações por meio de mecanismos como os Cookies ultrapassa a simples personalização de conteúdos e anúncios, tornando-se instrumento de monitoramento contínuo, construção de perfis comportamentais e influência sobre as escolhas dos indivíduos. Nesse contexto, o conceito de Data Totalitarianism evidencia o risco de erosão da esfera privada quando o tratamento de dados ocorre de forma permanente, opaca e em larga escala, permitindo que empresas detenham elevado poder sobre o comportamento de milhões de usuários. Diante desse cenário, o Data Protection by Design, posteriormente incorporado ao artigo 25 do GDPR, apresenta-se como uma resposta jurídica voltada à prevenção desses riscos, ao exigir que a proteção dos dados pessoais seja incorporada desde a concepção dos sistemas tecnológicos. Ao deslocar a proteção para a fase de desenvolvimento das tecnologias, o instituto fortalece a efetividade dos direitos fundamentais, reduz a dependência exclusiva do consentimento do usuário e impõe aos controladores o dever de estruturar sistemas compatíveis com os princípios da proteção de dados.

Palavras-chave: Mireille Hildebrandt; Data Protection by Design; Cookies; Totalitarismo de Dados.

REFERÊNCIA: HILDEBRANDT, Mireille; TIELEMANS, Laura. **Data protection by design and technology neutral law.** *Computer Law & Security Review*, Amsterdam, v. 29, n. 5, p. 509-521, 2013. DOI: 10.1016/j.clsr.2013.07.005.

SHAKIL, Ismail. **Facebook suspende Cambridge Analytica por violação de políticas.** *GI*, 17 mar. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/facebook-suspende-cambridge-analytica-por-violacao-de-politicas.ghtml>. Acesso em: 8 set. 2026.

THE ALAN TURING INSTITUTE. *The Primitives of Legal Protection against Data Totalitarianisms: Professor Mireille Hildebrandt*. YouTube, 28 maio 2018. Disponível em: https://www.youtube.com/watch?v=woy7_L2JKC4. Acesso em: 7 set. 2026.

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 (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, L 119, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 8 set. 2026.

Juliana Santolin de Lima, Discente na Universidade do Estado de Minas Gerais, juliana.2511001720@discente.uemg.br.

Vinicius Fernandes Ormelesi, Docente na Universidade do Estado de Minas Gerais, vinicius.ormelesi@uemg.br