A privacidade como pilar da Infosfera: desafios frente à coleta massiva de dados

Abimael Ortiz Barros, Katiucia Fernanda Ribeiro Batista de Castilho, William Rodrigo Joanico, Natacia Regina Fidelis Marinho Ferraz, Diogenes Matos Padilha Ferraz

Universidade Federal do Paraná - UFPR

Palavras-chave: privacidade, infosfera, proteção de dados, capitalismo de vigilância, ética da informação

A sociedade atual está vivenciando uma mudança significativa no que diz respeito ao valor da informação e ao seu impacto em nossas vidas. O termo "Infosfera" (Floridi, 2014) se refere ao universo que envolve tudo relacionado à informação, incluindo seu impacto, como ela interage e seus processos. A privacidade é fundamental neste ambiente informacional, vai além da idéia tradicional de um “direito de estar só", como propuseram Warren e Brandeis (1890). Com o passar do tempo, o conceito de privacidade evoluiu para incluir questões mais intricadas de controle sobre informações. Nissenbaum (2009), por exemplo, sugere que é preciso considerar a “integridade contextual", isso significa que a privacidade tem a ver com o respeito às normas e expectativas que existem em diferentes círculos sociais sobre como as informações são compartilhadas e utilizadas. Com o auxílio de tecnologias avançadas, como big data e inteligência artificial, está ocorrendo uma coleta massiva de informações sobre as pessoas. Isso gerou uma grande disparidade no acesso à informação, colocando as pessoas em uma posição desfavorável. De acordo com um estudo de Solove (2021), as pessoas têm dificuldade em compreender, acompanhar e gerenciar o uso de suas informações pessoais. Zuboff (2019) teoriza o "capitalismo de vigilância" como um novo modelo econômico que extrai valor através da conversão de experiências humanas em dados comportamentais. Este sistema opera mediante a coleta ubíqua de informações pessoais, que são processados para criar "produtos de previsão comportamental" comercializados em mercados especializados. O que há de interessante nesses modelos é que eles vão além de apenas coletar dados, esses modelos exercem influência sobre o que as pessoas vão fazer. Tudo isso é feito por meio de técnicas específicas, como fazer as coisas mais personalizadas ou usar o que se chama de nudging (Yeung, 2017). A questão mais importante aqui é como essa dinâmica altera nossa compreensão da privacidade. Anteriormente, era considerada um direito individual; atualmente, é percebida como um bem coletivo. A lógica extratora do capitalismo de vigilância estabelece uma economia política da informação pessoal na qual os indivíduos fornecem dados como "trabalho gratuito" sem compreender plenamente as implicações deste processo (Fuchs, 2014). Esta assimetria informacional manifesta-se tanto na opacidade dos algoritmos quanto na complexidade dos termos de serviço, criando condições estruturais para a exploração de dados pessoais.

Fundamentação na literatura

Luciano Floridi (2013) argumenta que a infosfera deve ser considerada um patrimônio comum e, como tal, deve ser administrada de maneira colaborativa. Essa concepção ultrapassa a maneira convencional de classificar as coisas como públicas e privadas. Ela admite que a qualidade do mundo da informação tem um impacto significativo na democracia, inovação e desenvolvimento humano. A ética da informação é um conceito que abrange não apenas as pessoas, mas também organizações e tecnologias. Essa visão mais ampla de responsabilidades morais faz com que consideremos também as interações que envolvem inteligência artificial e sistemas automatizados, e como elas afetam a forma como lidamos com as informações. A disseminação de informações falsas, a manipulação dos algoritmos e a vigilância em massa estão desgastando a forma como obtém e processamos informações, colocando em risco não apenas os direitos individuais, mas também a própria estrutura que permite o funcionamento de sociedades democráticas. Isso foi apontado por (Tufekci, 2014). Quanto aos marcos regulatórios, importante ressaltar que, na última década houve importantes avanços na criação de regras para proteger informações pessoais. A União Europeia, por exemplo, criou em 2016 o Regulamento Geral sobre Proteção de Dados (GDPR, 2016), e o Brasil, em 2018, promulgou a Lei Geral de Proteção de Dados (LGPD, 2018).

O estabelecimento de responsabilidade jurídica clara e mecanismos sancionatórios representa avanço significativo na proteção de direitos informacionais. Entretanto, há limitações importantes. As regras não se aplicam bem fora do território, principalmente quando se tratam de plataformas globais sediadas em países com leis de proteção de dados mais frouxas (Bradford, 2020). As leis atuais que protegem os dados têm um grande problema com a ideia do consentimento. Ele surge de uma ideia errada de que as pessoas têm controle sobre o que acontece com seus dados. Solove (2013), descreve isso como a “ilusão de controle". Um problema é gerado pela letra pequena dos termos de serviço e das políticas de privacidade. McDonald e Cranor (2008) estimaram que um usuário médio gastaria cerca de 244 horas por ano lendo todas as políticas de privacidade dos serviços que utiliza. Isso demonstra que é quase inviável continuar como se faz atualmente. Obar e Oeldorf-Hirsch (2020) mostram que a maior parte das pessoas concorda com os termos de serviço sem nem mesmo lê-los. Isso é algo que eles chamam de “a maior mentira da internet".A forma como coletamos dados está mudando drasticamente a maneira como vivemos. Isso acaba criando um ambiente em que todos podemos ser vigiados o tempo todo, o que é conhecido como vigilância panóptica. Foucault (1977) usou a ideia de uma prisão chamada panopticon para descrever como as sociedades funcionam quando as pessoas acham que podem ser vigiadas a qualquer momento. Penney (2016) demonstra como a revelação de programas de vigilância em massa afeta o comportamento das pessoas na internet. Quando esses programas são expostos, as pessoas passam a procurar menos por informações sensíveis, mostrando um impacto negativo sobre a liberdade de expressão e o acesso à informação. Esse efeito, conhecido como “efeito de resfriamento", é quando as pessoas se autocensuram

por medo de estar sendo monitoradas. A vigilância de hoje é diferente do modelo tradicional conhecido como panóptico. Ela usa várias técnicas para prever como as pessoas vão se comportar no futuro e, baseada nisso, influenciar esses comportamentos. Trata-se de uma forma de gestão mais sutil, que não se baseia apenas em regras e punições, mas que muda a maneira como as pessoas tomam suas decisões, alterando o ambiente ao seu redor Rouvroy (2013). O desenvolvimento de tecnologias de proteção da privacidade oferece alternativas técnicas para mitigar riscos associados à coleta massiva de dados. Técnicas criptográficas como criptografia homomórfica e computação segura multipartidária permitem processamento de dados preservando privacidade (Gentry, 2009). Cavoukian (2009) apresentou um conceito chamado “Privacy by Design", uma abordagem proativa que visa incluir proteções de privacidade já nas fases iniciais de desenvolvimento. Esse modelo estabelece sete princípios fundamentais: ser proativo, ter a privacidade como opção padrão, incorporar a privacidade no design, dar acesso completo, garantir a segurança em todos os pontos, oferecer transparência e visibilidade, além de respeitar a escolha do usuário quando se trata de privacidade. As redes descentralizadas e a tecnologia blockchain proporcionam maneiras novas de organizar o controle de dados. Por exemplo, estudos mostram que essa descentralização pode ser uma resposta aos modelos atuais, que muitas vezes concentram o controle nas mãos de poucos (Zyskind et al., 2015).

Relevância da pesquisa para a gestão da informação na esfera pública

O estudo atual é essencial para o domínio da gestão da informação no setor de administração pública dada a série de desafios que as entidades governamentais enfrentam ao lidar com a salvaguarda de dados pessoais dos cidadãos em meio a um cenário de rápida digitalização. Compreender a privacidade como um elemento fundamental do ambiente informacional torna-se imprescindível para gestores públicos que buscam equacionar a transparência governamental, a eficácia dos serviços online e a segurança dos direitos informáticos da população.

Objetivos do trabalho

O objetivo principal deste estudo é analisar os atuais desafios da privacidade na era da informação diante da coleta extensiva de dados e investigar de que forma a vigilância capitalista afeta a segurança das informações pessoais.

Procedimentos metodológicos, resultados e discussões

A pesquisa adotou abordagem qualitativa baseada em revisão bibliográfica sistemática, analisando marcos teóricos interdisciplinares (Floridi, Zuboff, Nissenbaum) e regulamentações contemporâneas (GDPR, LGPD). Os resultados: identificaram três achados centrais: a emergência do capitalismo de vigilância como sistema que transforma experiências humanas em dados comercializáveis; a inadequação dos

mecanismos de consentimento informado; e a necessidade de reconceptualizar privacidade como bem coletivo. Discussões: A privacidade na era digital transcende questões de direitos individuais para constituir-se como requisito fundamental para a preservação da infosfera como bem comum. A análise apresentada revela que as ameaças contemporâneas à privacidade, particularmente através do capitalismo de vigilância e da coleta massiva de dados, estabelecem riscos sistêmicos para a autonomia individual e a democracia. As leis de proteção de dados atuais são um grande passo adiante, mas não bastam para lidar com as coisas complicadas que acontecem quando se fala em informação e dinheiro. Uma dessas coisas problemáticas é a ideia de consentimento informado, ela tem problemas tanto teóricos quanto práticos. A ideia de Floridi sobre a ética na infosfera traz uma abordagem interessante para lidar com os problemas que surgem com a informação hoje. Ele destaca como esses desafios informacionais são questões de todos, não apenas individuais. O futuro da privacidade na infosfera está diretamente ligado à nossa capacidade de criar regras claras para o uso da informação. Precisamos achar um meio de equilibrar o avanço tecnológico com a proteção dos direitos básicos das pessoas. Isso garantirá que a internet e outras tecnologias sirvam para melhorar a vida humana e apoiar a democracia, em vez de miná-la devagar.

Contribuições e implicações para o desenvolvimento do conhecimento

A pesquisa contribui teoricamente ao integrar perspectivas filosóficas, econômicas e técnicas na análise da privacidade digital, aplicando o conceito de infosfera ao contexto da gestão pública. Praticamente, oferece subsídios para políticas públicas mais efetivas de proteção de dados e implementação de princípios de "privacy by design" em sistemas governamentais. As implicações para pesquisas futuras incluem a necessidade de investigações empíricas sobre efetividade de soluções tecnológicas em contextos públicos e desenvolvimento de modelos alternativos de governança de dados que transcendam o paradigma do consentimento individual.

Referências

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.

Floridi, L. (2013). The ethics of information. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001

Floridi, L. (2014). The fourth revolution: How the infosphere is reshaping human reality. Oxford University Press.

Foucault, M. (1977). Discipline and punish: The birth of the prison. Pantheon Books.
Fuchs, C. (2014). Digital labour and Karl Marx. Routledge. https://doi.org/10.4324/9781315880075

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169-178).

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4, 543-568.

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147.

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. Berkeley Technology Law Journal, 31(1), 117-182.

Rouvroy, A. (2013). The end(s) of critique: Data behaviourism versus due process. In M. Hildebrandt & K. De Vries (Eds.), Privacy, due process and the computational turn (pp. 143-167). Routledge.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126, 1880-1903.

Solove, D. J. (2021). Understanding privacy. Harvard University Press.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. First Monday, 19(7).

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193-220. https://doi.org/10.2307/1321160

Yeung, K. (2017). Hypernudge: Big data as a mode of regulation by design. Information, Communication & Society, 20(1), 118-136.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE security and privacy workshops (pp. 180-184). https://doi.org/10.1109/SPW.2015.27