Terêncio
ISSN: XXXX-XXXX

A VULNERABILIDADE DA PRIVACIDADE: QUEM REALMENTE CONTROLA SEUS DADOS?

A segurança das informações pessoais é ameaçada por grandes corporações no ambiente digital, levantando questões éticas sobre o controle das nossas informações

Beatriz Vernacci Antonio
Catharina Victoria Guerra
Rafaella Tessarotto de Menezes
Curso de Engenharia
Centro Universitário FEI

Palavras-chave: privacidade online; proteção de dados; tratamento de dados

Com a crescente coleta de dados pessoais por empresas e plataformas digitais, o uso indevido dessas informações tem se tornado uma ameaça constante à privacidade dos usuários.

A segurança das informações pessoais está cada vez mais em risco em um universo digital dominado por grandes corporações, criando dúvidas éticas sobre quem detém o poder de acessar, manipular e obter lucro com os dados pessoais de quem acessa a internet. Na era digital, na qual algoritmos decidem desde o que consumimos até nossas interações sociais, a questão da privacidade dos nossos dados torna-se cada vez mais urgente. Até que ponto esses dados estão seguros e qual o impacto disso na nossa cidadania digital?

A falta de transparência e consentimento no manuseio de dados coloca em risco a segurança individual. As informações pessoais, como hábitos de consumo, localização, e até mesmo dados financeiros, tornam-se vulneráveis, especialmente com o crescimento do uso de tecnologias que rastreiam o comportamento dos usuários sem que estes tenham plena consciência disso.

Muitos dos usuários desconhecem a profundidade com que suas atividades *online* estão sendo monitoradas. Termos de uso longos e complexos dificultam a compreensão dos direitos dos usuários, resultando em um consentimento passivo e muitas vezes inconsciente. O que muitas

ISSN: XXXX-XXXX

pessoas não percebem é que, ao aceitar esses termos, elas estão cedendo o controle sobre seus próprios dados para essas empresas.

A vulnerabilidade dos dados não está apenas na sua coleta, mas também no armazenamento. Muitas empresas têm acesso a uma grande quantidade de dados, os quais, em sua maioria, são adquiridos sem o consentimento claro dos indivíduos. Gigantes da tecnologia, como Google e Amazon, são frequentemente acusadas de utilizar esses dados para obter vantagens em meios comerciais. O uso de sistemas sofisticados não só permite às empresas personalizarem anúncios, mas também predizer e manipular o comportamento dos usuários.

Assim, escândalos envolvendo vazamento de dados têm se tornado comuns nos últimos anos, como o caso amplamente divulgado da Cambridge Analytica, no qual a empresa utilizou dados de milhões de usuários do Facebook, sem consentimento, para influenciar campanhas políticas, impactando nas eleições presidenciais dos Estados Unidos e o referendo do Brexit (BBC BRASIL, 2018; CLARKE, 2020). Isso comprova como a falta de transparência no uso de dados digitais pode ser perigoso nas decisões que envolvem países inteiros. Além de ter revelado como a privacidade dos usuários pode ser facilmente violada também para finalidades políticas.

Esse incidente expôs uma atividade muito comum que as grandes empresas têm que o poder de utilizar os dados pessoais da população, sem o consentimento explicito do usuário, de forma não ética, beneficiando as empresas e seus donos, e influenciando diretamente ou indiretamente nas decisões importantes para a política de seus países. Isso levanta a questão de até que ponto os indivíduos têm uma verdadeira autonomia para tomar decisões conscientes estando no mundo digital.

Mais do que ameaçar a privacidade, os vazamentos de dados abrem brechas para crimes como roubo de identidade e fraude financeira. Criminosos podem usar informações aparentemente inofensivas para cometer crimes de maneira silenciosa e quase indetectável.

Em resposta à essa questão, a regulação do uso de dados pessoais se tornou uma preocupação global. Consequentemente, a União Europeia implementou o Regulamento Geral de Proteção de Dados (GDPR) em 2018, que exige o consentimento explícito dos usuários e garante direitos como o esquecimento e a portabilidade (EUROPEAN COMMISION, s/d.). No Brasil, a Lei Geral de Proteção de Dados (LGPD), inspirada no GDPR, entrou em vigor em 2020, estabelecendo regras sobre coleta, armazenamento e compartilhamento de dados, além de impor sanções rigorosas para quem descumprir as normas, marcando um avanço na proteção da privacidade digital (BRASIL, 2018).

Com isso, devemos questionar se as grandes empresas realmente respeitam nossa privacidade e pensam em nossa segurança no meio tecnológico, ou se para elas o importante seja só lucrar em cima de quem usufrui de suas plataformas. Embora o uso de dados seja, em muitos casos, coletado para a personalização de serviços e desenvolvimento de novos aplicativos, ele também deixa claro o quão vulnerável é privacidade desses usuários e o quão fácil é acessá-la. A pressão para que os dados pessoais sejam melhor protegidos e usados apenas com a aprovação total de seus donos tem feito com que as grandes empresas tentem resolver o real desafio, que é a implementação de práticas que priorizem e melhorem a proteção dos dados, além de respeitarem à privacidade dos usuários (MARTINS, 2024).

Por fim, podemos concluir que com o avanço nos modos em que os dados são coletados, é essencial que as corporações parem de usar as informações pessoais no meio digital para fins próprios, já que é inadmissível que os usuários não tenham conhecimento claro sobre como suas informações pessoais podem estar sendo usadas devido à falta de transparência dessas empresas. Além do fato de que, como falado anteriormente, esses dados podem ser usados para manipular os usuários sem nem mesmo eles perceberem, podendo influenciar, em larga escala, até em decisões políticas de um país inteiro.

Referências

BBC BRASIL. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC BRASIL**, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: out. 2024.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**, Lei nº 13.709/2018.

CLARKE, Laurie. How the Cambridge Analytica scandal unravelled. The New Statesman, 15 out. 2020. Disponível em: https://www.newstatesman.com/long-reads/2020/10/how-cambridge-analytica-scandal-unravelled. Acesso em: out. 2023.

EPOCA NEGÓCIOS ONLINE. O que Mark Zuckerberg tem a dizer sobre o escândalo de uso de dados. **Época Negócios Online**, 05 abr. 2018. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2018/04/o-que-mark-zuckerberg-tem-dizer-sobre-o-escandalo-de-uso-de-dados.html. Acesso em: out. 2024.

EUROPEAN COMMISSION. **Data protection**. s/d. Disponível em: https://commission.europa.eu/law/law-topic/data-protection_en. Acesso em: out. 2024.

MARTINS, Antônio Eduardo Senna. Os Desafios da Proteção de Dados Pessoais na Era Digital. **Jusbrasil**, 2024. Disponível em: https://www.jusbrasil.com.br/artigos/os-desafios-da-protecao-de-dados-pessoais-na-era-digital/1971809645?utm_medium=social&utm_campaign=link. Acesso em out. 2024.

ISSN: XXXX-XXXX

SOUZA, Ramon de. O que são data brokers e como eles funcionam? **Canaltech**, 05 fev. 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-sao-data-brokers-e-como-eles-funcionam-176757/. Acesso em: out. 2024.