REVISTA DE DIREITOS HUMANOS
E DESENVOLVIMENTO SOCIAL

ORIGINAL

Resultado do II Congresso Internacional de proteção de Dados Pessoais e Direitos Humanos

Editores
Fernanda Carolina Araújo Ifanger e Lucas Catib De Laurentiis

Conflito de interesses
Os autores declaram não haver conflito de interesses.

Recebido
23 jul. 2024

Aprovado
23 jul. 2024

LGPD e o setor público: uma análise sobre os riscos para os usuários ao utilizar-se de mídias sociais para identificação em sistemas informatizados governamentais

LGPD and the public sector: an analysis of the risks for users when using social media for identification in government computer systems

Beatriz Christina Martins Norbiato[1], Teresa Christina Pinto Machado da Silva[1]

[1] Pontifícia Universidade Católica de Campinas (PUC-Campinas), Escola de Ciências Humanas, Jurídicas e Sociais, Faculdade de Direito. Campinas, SP, Brasil. Correspondência para: B. C. M. NORBIATO. *E-mail:* <bia.cm.norbiato@gmail.com>.

Artigo elaborado a partir de resumo apresentado no II Congresso Internacional de Proteção de Dados Pessoais e Direitos Humanos, realizado em Campinas em novembro de 2024.

Como citar este artigo: Moreira, A. E.; Silva, T. H. B.; Santos, T. M. LGPD e o setor público: uma análise sobre os riscos para os usuários ao utilizar-se de mídias sociais para identificação em sistemas informatizados governamentais. *Revista de Direitos Humanos e Desenvolvimento Social*, v. 5, e2413771, 2024. https://doi.org/10.24220/2675-9160v5a2024e13771

Resumo

O presente estudo tem como objetivo analisar os riscos de vazamento de dados aos quais os usuários estão expostos ao utilizar-se de mídias sociais para identificação em sistemas informatizados governamentais, além de expor a fragilidade desses sistemas por falta de investimentos públicos para reforçar sua segurança. Possui também o objetivo de apresentar o papel das políticas de privacidade nos sistemas de informações tanto no Brasil, quanto em sistemas privados e a exigência legal da proteção de dados por meio de Leis e Normas previstas pela Constituição Federal e por seus respectivos dispositivos vigentes no país. Com isso, a pesquisa preocupa-se em explorar o questionamento de que os indivíduos que utilizam de suas contas em redes sociais para se cadastrar nos sites oferecidos pelo governo estão seguros ou se colocam em riscos mais do que usuários que não unificam suas contas sociais.

Palavras-chave: LGPD. Marco civil da internet. Riscos aos usuários. Sistemas de informação governamentais. Vazamento de dados.

Abstract

The present study aims to analyze the risks of data leaks to which users are exposed when using social media for identification in government information systems, as well as to expose the vulnerability of these systems due to lack of investments in strengthening their security. It also aims to present the role of privacy policies in information systems and the legal requirement for data protection through laws and regulations provided both by the Federal Constitution and by

their respective provisions in force in the country. Therefore, the research is concerned with exploring the question of whether individuals who use their social media accounts to register on websites offered by the government are secure or if they are at greater risk than users who do not link their social accounts.

Keywords: *LGPD. Marco civil framework . Risks to internet users. Governament information systems. Data leak.*

Introdução

A internet teve seu início como um projeto militar nos Estados Unidos denominado APARNet, desenvolvido pela *Advanced Research Projects Agency* (ARPA, Rede de Agências de Projetos de Pesquisa Avançada) na década de 1960. O objetivo inicial era criar uma rede de comunicação descentralizada e resistente a falhas, capaz de manter a comunicação em caso de ataques durante a Guerra Fria. Assim, em 1969 surgiu a primeira conexão entre computadores da University Stanford e da University of California, Los Angeles (UCLA).

Ao longo das décadas seguintes, a internet evoluiu, expandiu-se para além de contextos militares e acadêmicos, tornando-se acessível para o público em geral. Atualmente, a sociedade contemporânea vive em uma era digital, onde a interconexão e o compartilhamento de informações são pilares fundamentais para o funcionamento de diversas atividades, dentre elas as governamentais.

Nesse sentido, a utilização de mídias sociais como ferramenta de identificação em sistemas informatizados governamentais tem se tornado uma prática cada vez mais comum. Sob esse viés, é possível indagar que essas formas federalizadas de identificação podem ocasionar riscos à segurança dos usuários, já que dados pessoais captados pelas mídias sociais são repassados a outros sistemas.

Assim, é possível perceber a importância do presente tema, que tem como objetivo analisar os possíveis riscos de vazamentos em sites do governo e os riscos aos quais os usuários estão expostos ao utilizar-se de mídias sociais para identificação em sistemas governamentais.

Ademais, o estudo também busca apontar o papel das políticas de privacidade nos sistemas de informação e a exigência legal de proteção de dados.

O presente artigo foi divido em quatro capítulos, e consiste em pesquisa bibliográfica e documental se valendo de artigos científicos e outras revisões bibliográficas, além de análises das legislações permitidas. Sendo fracionado da seguinte forma: o primeiro capítulo tratará a respeito das mídias sociais, sendo abordado um pouco de seus conceitos básicos, como sua definição e seu modo de funcionamento. No segundo capítulo será abordado os principais motivos de se utilizarem as mídias sociais para a identificação de sistemas governamentais. No decorrer do terceiro capítulo será elencado os possíveis riscos da utilização de mídias sociais para a identificação de sistemas governamentais, bem como as consequências desse ato para a segurança pública. Durante o quarto capítulo será realizada uma análise da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e do Marco Civil da internet sob a luz dessa problemática, além de buscar ressaltar a importância de tais dispositivos na sociedade contemporânea.

Por fim, serão apresentadas as considerações finais, na expectativa que o constante debate do tema reforce a sua relevância.

Redes sociais: uma análise abrangente

A *priori*, devemos fazer uma análise a respeito das redes sociais, a fim de compreender melhor o funcionamento de um de nossos principais objetos de estudo.

As redes sociais têm uma história que remonta ao ano de 1995, quando Randy Conrads criou o site <classmates.com>, que tinha como objetivo a interação de seus usuários com antigos companheiros de escola para recuperar ou manter contato. No entanto, foi a partir dos anos 2000 que foi possível observar um crescimento desse tipo de plataformas, se tornando uma parte integrante da vida cotidiana de um número crescente de pessoas. Contudo, definir de forma precisa e estática o conceito de redes sociais se torna uma tarefa desafiadora devido a sua natureza mutável ao longo do tempo e a emergência de novas plataformas.

No cerne da definição, consideramos redes sociais como serviços baseados na web que possibilitam aos usuários construírem perfis públicos ou semipúblicos, articular listas de conexões e interagir com outros usuários dentro do sistema. Essa interação individual é o cerne dessas plataformas, independentemente de suas características específicas e do tipo de conexões estabelecidas. Sob esse viés, é possível perceber que o objetivo dessas redes, independente da forma como utilizada perante o seu usuário, é o de conectá-lo a um grande número de pessoas, possibilitando a interação individual entre indivíduos.

Nesse sentido, considerando a amplitude do conceito de rede social, surgem diversas designações de acordo com o foco da rede, sendo as mais relevantes as próprias ou generalistas e as impróprias.

Uma rede social pode ser denominada de própria ou generalista quando seu principal foco for a formulação de perfis públicos e individuais que permitam a interação entre os usuários. Outras características dessa rede social são a existência de uma gama de funcionalidades diferentes, o que fornece aos seus usuários uma plataforma que integre diversas ferramentas em um mesmo lugar, e impulsionam uma interação que ultrapasse o âmbito online e que possa se concretizar na vida cotidiana. Um exemplo dessa modalidade de rede é o Facebook e o X (antigo Twitter).

Paralelamente, há também as redes sociais denominadas como impróprias, que seriam aquelas que funcionam como um apêndice de outro serviço ou ferramenta, gravitando e existindo em função deste. Essas redes impróprias podem ofertar um conjunto parcial de ferramentas típicas de interação encontradas nas redes sociais próprias, e podem ser mencionadas como exemplos as redes sociais presentes em sites de comércio eletrônico, como Mercado Livre e Ebay, ou sites que têm como objetivo primordial o intercâmbio de conteúdo e não propriamente a interação social, mas que também cultivam suas próprias comunidades de usuários, como o Youtube.

Dentro das redes sociais impróprias, destacam-se duas categorias de extrema relevância. Uma delas é a das redes sociais estruturadas em torno do intercâmbio de conteúdo. Sendo este, geralmente, alguma espécie de mídia eletrônica, tais como documentos e apresentações, vídeos, entre outros. Sendo assim, vale destacar que a utilização de ferramentas típicas de redes sociais pode aumentar a eficácia deste intercâmbio de conteúdo, através da formação de comunidades de interesses específicos e do intercâmbio de opiniões críticas, por exemplo.

A outra subcategoria corresponde às redes sociais que possuem o foco em relacionamentos profissionais. Estas são chamadas de redes sociais de conteúdo profissional, e se configuram como novas ferramentas de ajuda para estabelecer contatos profissionais com outros usuários.

A sustentabilidade das redes sociais e a complexidade das relações contratuais

Uma vez finalizada a análise a respeito do conceito, passaremos agora a tratar da relação que o usuário possui com a rede social. Em grande parte, esses serviços são oferecidos gratuitamente aos usuários, o que naturalmente suscita questionamentos sobre como tais plataformas conseguem

sustentar suas operações, especialmente considerando a magnitude de suas infraestruturas e o constante desenvolvimento de novos recursos.

A análise da sustentabilidade de uma rede social pode ser dividida em duas fases distintas. Na primeira fase, a ênfase recai sobre a expansão da base de usuários, buscando não apenas a ampliação quantitativa, mas também a fidelização, incentivando a utilização diária e a manutenção de perfis atualizados. Já na segunda fase, a plataforma busca monetizar sua base de usuários, sendo a publicidade o modelo de exploração mais comum. A utilização estratégica dos dados dos usuários permite que as redes sociais ofereçam publicidade direcionada, gerando receitas provenientes de empresas que pagam pela promoção de suas marcas.

Ao se cadastrar nas redes sociais o usuário realiza contratos para poder estar dentro dessas plataformas. Sendo assim, este se torna um consumidor, pois está utilizando um serviço oferecido por empresas. Juridicamente, a jurisprudência reconhece que essas plataformas atuam na gestão de dados e na disponibilização de acesso por meio de links, se enquadrando como provedores de hospedagem, e, portanto, sujeitos do regime de responsabilidade civil correspondente.

A relação de consumo entre usuário e rede social é caracterizada pela existência de um contrato, sendo o mais comum o de adesão. Esse tipo de contrato implica que uma das partes deve aceitar, de forma integral, às cláusulas estabelecidas pela outra, aderindo a uma situação contratual definida em todos os seus termos. Todavia, essa adesão ocorre de forma unilateral colocando as partes em uma situação de desigualdade, em que os interesses do fornecedor predominam sobre os do consumidor.

Sob esse viés, uma das principais problemáticas relacionadas aos contratos de adesão nas redes sociais reside na dificuldade de modificação das cláusulas gerais. Frequentemente, não há mecanismos que permitam aos usuários proporem alterações, o que reforça a assimetria de poder entre as partes envolvidas.

Em suma, a sustentabilidade das redes sociais envolve uma complexa interação entre a expansão da base de usuários, a monetização por meio de publicidade e os contratos de adesão que regulam a relação entre usuários e plataformas.

O papel das redes sociais na identificação de sistemas governamentais

É fato que o advento da tecnologia da informação e a disseminação da internet têm transformado a maneira como os governos interagem com a população. No Brasil, é possível observar um movimento significativo em direção a criação de websites governamentais que tem como objetivo promover a participação cidadã e a transparência nas ações do governo, especialmente em níveis municipais e estaduais.

No âmbito municipal, o Orçamento Participativo Digital (OP Digital) desponta como um exemplo pioneiro de envolvimento da população nas decisões políticas locais. Desenvolvido com o auxílio da internet, esse sistema permite que os cidadãos opinem em projetos, influenciem a priorização de políticas públicas e monitorem a execução física e orçamentária dessas iniciativas. Já em nível estadual, a criação de portais de governo visa facilitar a comunicação entre a administração pública e a população.

O conceito de governo aberto, também conhecido como *open government*, ressalta a importância do acesso à informação governamental como um direito da população (Queiroz; Motta, 2017). A transparência visa permitir que os cidadãos fiscalizem, cobrem e responsabilizem o governo pelo uso adequado dos recursos públicos. Essa abordagem se materializa na forma de

"dados governamentais abertos" (*open government data*), detalhado pela *Open Definition* em 2005, tornando-se uma prática adotada por governos em busca de transparência.

Nesse sentido, o uso generalizado de redes sociais, como Facebook e ferramentas do Google, para autenticação em sistemas, incluindo governamentais, é uma prática comum devido à popularidade dessas plataformas no Brasil. Essa abordagem federativa, discutida por Wangham, Santos e Moreira (2022), é apontada como uma tendência na gestão de identidades.

Entretanto, o uso dessas formas federalizadas de identificação levanta preocupações relacionadas à privacidade dos cidadãos. Isso ocorre, visto que, como abordado anteriormente no decorrer do artigo, os dados pessoais captados pelo Facebook e pelo Google são repassados a outros sistemas, representando um desafio significativo para a segurança da informação.

Assim, fica evidente que a interseção entre governo eletrônico, dados abertos e privacidade dos cidadãos ressalta a necessidade de abordagens cuidadosas na implementação de políticas e práticas governamentais. O equilíbrio entre transparência e proteção de dados pessoais emerge como um desafio crucial para o avanço bem-sucedido do governo digital no Brasil, bem como em outras partes do mundo. O próximo passo é analisar os desafios que essa prática acarreta juntamente de políticas públicas e soluções para melhorar o problema.

Riscos da utilização de mídias sociais para a identificação em sites governamentais e consequências para a segurança pública

É verdade que a coleta de dados pessoais em sites e mídias sociais é uma preocupação para os usuários. Ao cadastrar-se em uma plataforma, é comum fornecer informações como nome, data de nascimento, e-mail e senha. Esses dados são essenciais para a criação e personalização da conta do usuário. A conta do Google é um exemplo de plataforma que coleta dados pessoais dos usuários. Com uma base de aproximadamente 1,5 bilhão de contas ativas (Montenegro, 2018), o Google oferece acesso fácil a diversas plataformas e recursos, como o preenchimento automático, que facilita o login em sites e dispositivos sem a necessidade de inserir manualmente as informações novamente. No entanto, é importante ressaltar que cada ação realizada pelo usuário, como visualizar, publicar, curtir ou pesquisar palavras, resulta na coleta e armazenamento de dados. Essas informações podem incluir padrões de comportamento, reações físicas e preferências do usuário, que acabam criando filtros de informações pessoais.

Embora essa coleta de dados seja usada para oferecer serviços personalizados e melhorar a experiência do usuário, também pode deixar as pessoas vulneráveis, uma vez que existem empresas que utilizam esses dados para fins comerciais. Existem plataformas clandestinas que funcionam dentro da *dark web* e em comunidades *crackers* que comercializam dados pessoais de forma ilegal e sem conhecimento do usuário após comprarem de empresas que prestam serviços ao público.

> Essas organizações se formam de forma quase empresarial, admitindo inscrições de hackers que em comunidade passam a atuar. Nesta semana, por exemplo, uma operação conjunta de diversas polícias europeias e dos Estados Unidos, divulgou a captura dos hackers que alimentavam o site RaidForums, onde milhões de dados eram vendidos (Saiba como funciona [...], 2022, *online*).

Existe também a possibilidade da obtenção de informações pessoais não autorizadas por meio de uma prática conhecida como engenharia social, uma atividade que analisa o comportamento social para descobrir senhas identificando denominadores comuns, citando como exemplo, uso de nomes, sobrenomes de pessoas conhecidas pelos usuários, datas de nascimento ou datas pessoais.

De acordo com Mitnick e Simon (2002), um engenheiro social, de forma geral, é um indivíduo que através da manipulação, conquista a confiança de sua vítima para ter acesso a informações privadas. Sendo assim, as informações que a vítima fornece podem ser utilizadas para lhe causar prejuízo de diversas formas, como financeiro, psicológico, social e empresarial (Cortella, 2013).

Os ataques indiretos têm como característica a utilização de outros meios para chegar ao seu objetivo, isso através de softwares ou ferramentas, por exemplo, vírus, sites falsos, cavalos de troia ou por e-mails falsos (*phishing*). Sendo assim, através desses meios o atacante pode obter as informações que deseja.

Riscos da utilização de mídias sociais para identificação em sistemas governamentais e consequências para segurança pública: estudo de caso

Ante ao exposto, notamos que, devido ao uso de mídias sociais, e até mesmo de sites necessários para serviços oferecidos pelo Estado, o indivíduo está sujeito a ter a sua privacidade violada por quebras de códigos dentro de sites.

Como o ocorrido no caso de um vazamento de dados, no ano de 2021, que expôs 220 milhões de brasileiros, incluindo falecidos, quando o sistema de dados do Departamento Estadual de Trânsito do Rio Grande do Sul (Detran-RS) e da secretaria de saúde de Goiás foi invadido (Steil, 2024).

O site da Secretaria de Saúde de Goiás já tinha sido alvo de uma exposição de dados anteriormente, tendo 240 milhões de senhas de pacientes vazadas. De acordo com Fábio Ramos, executivo-chefe da empresa antifraudes Axur, "os governos brasileiros erram na manutenção da segurança digital de seus serviços, especialmente se comparado ao trabalho de grandes empresas privadas" (Tagiaroli, 2021, *online*).

Os órgãos públicos são muito visados em ciberataques por motivos como possibilidade de acesso a um vasto banco de dados; rápida monetização de dados obtidos; baixo investimento em segurança da informação por parte do governo, etc.

Neste caso, vale ressaltar que o site do Detran, independente do Estado pertencente, é intrínseco ao Portal Único Gov.br, que reúne no mesmo sistema serviços para o cidadão e informações, como discutido previamente no artigo.

No caso deste vazamento, fora liberado dados sobre os donos dos veículos, bem como, modelo, ano, placa, renavam, colocando em risco os motoristas e seu patrimônio, uma vez que suas informações poderiam ter sido acessadas facilmente.

Para acessar o Portal é necessário fazer um cadastro, onde diversos usuários, pela facilidade, utilizam-se de suas redes sociais para fazer registro, e com isso, correm perigos anteriormente relacionados, ou seja, usuários que conectam suas contas podem se tornar mais suscetíveis a ter diversos dados vazados.

LGPD e marco civil da internet

Diariamente usuários se conectam em suas redes sociais pelos mais diversos motivos, e, por mais que não estejam completamente seguros com suas informações pessoais sendo utilizados por essas plataformas e todos esses dados estejam salvos em banco de dados como apresentado ao decorrer do artigo, existe sim, leis que protegem esses indivíduos e sua privacidade.

O Marco Civil da Internet, Lei nº 12.965/14, é uma lei que estabelece princípios para tornar a internet mais segura e democrática, tendo como princípio regular os direitos, garantias e deveres do uso da internet.

Segundo Damásio de Jesus (2014), a criação do Marco Civil para o direito brasileiro era gerar uma normatização específica ao Poder Judiciário como resolução de problemas que envolvessem a internet, de forma que se evitasse decisões jurídicas contraditórias sobre o tema.

Apesar de termos a sensação de que a internet é uma "terra sem lei", esse sentimento está equivocado. Antes do Marco Civil da Internet não existia uma legislação específica acerca do tema, o direito se utilizava para tratar sobre essas problemáticas o Art. 5 da Constituição Federal,

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Brasil, 1988, online).

No entanto, após 2014, foi integrado à nossa legislação a Lei nº 12.965, que conta com 32 artigos e dentre eles garantias de liberdade de expressão, comunicação, proteção à privacidade e dados pessoais, responsabilidades, dentre outros.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II – proteção da privacidade (Brasil, 2014, *online*).

Neste mesmo parâmetro, o Art. 7º da mesma lei traz exigência de consentimento livre e por parte do usuário, assim como dos direitos de inviolabilidade da intimidade e da vida privada.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei
>
> (Brasil, 2014, *online*).

Outro ponto feito pelo Marco Civil da Internet, em seu Art. 19º, é o respeito à relação entre o direito à liberdade de expressão e a responsabilização subjetiva dos provedores de aplicação de internet:

> Art. 19º. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (Brasil, 2014, *online*).

Além disso, o Art. 8º da mesma Lei dispõe sobre o consentimento livre, informado e inequívoco, que deve ser fornecido por escrito ou por algum meio que demonstre manifestação de vontade do titular dos dados; e o Art. 9ª determina que as empresas devem informar aos titulares dos dados sobre o propósito da coleta, bem como sua utilização.

A proteção de dados é fundamental quando se trata de direitos da personalidade, tendo como principal objetivo analisar a natureza jurídica e os limites da responsabilidade civil de usuários e fornecedores que lidam com dados no Brasil.

Além disso, ao apresentarmos dispositivos jurídicos sobre a utilização das redes, é importante ressaltar que não contamos apenas com o Marco Civil, mas também com princípios, como o princípio da razoabilidade e da proporcionalidade, a própria Constituição Federal e a Lei Geral de Proteção de Dados. Neste contexto, também surge a Lei Geral da Proteção de Dados, lei n° 13.709, aprovada em agosto de 2018, com vigência a partir de agosto de 2020.

A LGPD tem como objetivo a proteção de dados dos cidadãos brasileiros e sua privacidade (Cartolari, 2019), isso se estende também à coleta desenfreada de dados por parte das plataformas sociais. A lei estipula e difere quais dados são pessoais, sensíveis e anônimos, além de definir quais podem ser coletados, armazenados, processados e compartilhados.

Os dados pessoais são aqueles que possibilitam a identificação do usuário de forma direta ou indireta, como exemplo, nome e apelido, endereço, endereço eletrônico, endereço de IP, telefone, dentre outros. Dados sensíveis são aqueles que estão sujeitos a condições específicas de tratamento, ou seja, exigem maior atenção, dentre eles, origem racial ou étnica, religião, opiniões políticas, filiação sindical, questões genéticas, biométricas e sexual do indivíduo. E, por fim, dados anonimizados, que são considerados por vias técnicas de processamento de dados ou outros meios impossíveis de se identificar o titular dos dados em questão, ou seja, dados que se desvinculam do seu dono (Justiça Federal, 2024).

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Brasil, 2018, *online*).

Para um dado se tornar público, a lei dispõe a possibilidade mediante o consentimento do titular,

> Art. 5° Para os fins desta Lei, considera-se:
>
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Brasil, 2018, *online*).

Bem como exposto pelo Art. 7° da mesma Lei, que trata:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

> I – mediante o fornecimento de consentimento pelo titular;
>
> (...)
>
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta lei (Brasil, 2018, *online*).

O controle do tratamento das informações deve ser papel do Estado, assim como a garantia de que seu uso não seja abusivo e que o direito à privacidade, previsto pela Constituição Federal, seja respeitado. Bem como o acesso dos indivíduos às suas próprias informações para que possa alterar ou remover os dados armazenados pela entidade. Além disso, criar regras para o caso de violações e a necessidade de transparência sobre os métodos usados para manipular os dados que foram oferecidos na internet, como apresentado por Maldonado (2019).

Assim como previsto pelo Art. 17º da Constituição Federal: "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei" (Brasil, 1988, *online*).

Com isso, é notório que os usuários estão amparados por leis e regulamentos, contudo, devem se atentar a forma com as quais utilizam suas redes sociais ou fazem seus logins em sites, para que assim, não se exponham a tantos outros riscos.

Considerações Finais

Diante do exposto no decorrer deste estudo, é perceptível que a análise abordada neste projeto revela a complexidade dos desafios enfrentados pela sociedade contemporânea diante da intersecção entre o uso generalizado de redes sociais e a integração dessas plataformas na identificação de sistemas governamentais.

O advento da internet trouxe consigo um mar de possibilidades, permitindo uma interconexão sem precedentes entre os indivíduos e os órgãos governamentais. No entanto, essa interconexão também expõe os usuários a uma série de riscos, especialmente relacionados à privacidade e à segurança dos dados pessoais. Ao longo deste estudo, é possível traçar a evolução das redes sociais, desde sua origem até sua integração cada vez maior na vida cotidiana da sociedade.

Ademais, também pode-se compreender a dinâmica dessas redes, bem como os modelos de negócios que sustentam essas plataformas, o que é crucial para realizar uma análise dos possíveis impactos da utilização dessas mídias na identificação de sistemas governamentais.

A prática comum de utilizar redes sociais para autenticação em sites governamentais traz à tona importantes questões relacionadas à segurança da informação e a privacidade dos cidadãos. Como demonstrado, os dados pessoais captados por essas plataformas podem ser repassados a outros sistemas, aumentando o risco de vazamentos e violações de privacidade. Além disso, o estudo identificou diversos tipos de riscos enfrentados pelos usuários, como a coleta indiscriminada de dados por empresas até os ataques cibernéticos direcionados aos órgãos governamentais.

Sob esse viés, se torna evidente a necessidade de abordagens cuidadosas na implementação de políticas e práticas governamentais relacionadas ao uso de redes sociais. O equilíbrio entre transparência e proteção de dados pessoais surge como um desafio crucial para o avanço bem-sucedido do governo digital. Nesse sentido, o Marco Civil da Internet e a Lei Geral de Proteção de Dados desempenham um papel fundamental na definição de diretrizes para o tratamento adequado dos dados dos indivíduos.

Por fim, este artigo ressalta a importância contínua do debate sobre essa temática, visando não apenas a compreensão dos desafios existentes, mas também a proposição de soluções e políticas públicas que promovam a segurança e a privacidade dos usuários em um cenário cada vez mais digitalizado.

Referências

Brasil. Constituição da República Federativa do Brasil. *Diário Oficial da União*: seção 1, Brasília, ano 126, n. 191-A, p. 2-32, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/DOUconstituicao88.pdf. Acesso em: 6 fev. 2024.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). *Diário Oficial da União*: seção 1, Brasília, n. 157, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 fev. 2024.

Brasil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, seção 1, Brasília, ano 151, n. 77, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 fev. 2024.

Cartolari, L. R. A Lei Geral de Proteção de Dados como ferramenta de proteção dos direitos fundamentais. *Repositório Institucional Univem*, 2019. Disponível em: https://aberto.univem.edu.br/handle/11077/1853. Acesso em: 6 fev. 2024.

Cortella, M. S. *Nos Labirintos da Moral*. São Paulo: Vozes, 2013.

Jesus, D. *Marco civil da internet*. São Paulo: Saraiva, 2014.

Justiça Federal. *Classificação dos Dados na LGPD*. *Justiça Federal 2ª Região*, Rio de Janeiro, 13 jun. 2024. Disponível em: https://www.trf2.jus.br/trf2/artigo/cinova/classificacao-dos-dados-na-lgpd. Acesso em: 6 fev. 2024.

Maldonado, V. N. *LGPD*: Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Revista dos Tribunais, 2019.

Mitnick, K.; Simon, W. L. *The Art of Deception*: *Controlling the Human Element of Security*. Indianapolis: Wiley Publishing, 2002.

Montenegro, P. Gmail ultrapassa 1,5 bilhão de usuários ativos ao redor do mundo. *TudoCelular.com*, [*S. l.*], 27 out. 2018. Disponível em: https://www.tudocelular.com/google/noticias/n132472/gmail-mais-de-1-5-bilhao-usuarios-ativos.html. Acesso em: 6 fev. 2024.

Queiroz, M. J.; Motta, G. H. M. B. Transparência e preservação de privacidade em dados governamentais no Brasil: pesquisa documental e estudo de caso. *Planejamento e Políticas Públicas*, v. 49, p. 431-465, 2017. Disponível em: https://www.ipea.gov.br/ppp/index.php/PPP/article/view/750. Acesso em: 6 fev. 2024.

Saiba como funciona a venda de dados pessoais na internet. *Migalhas*, [*S. l.*], 23 abr. 2022. Disponível em: https://www.migalhas.com.br/quentes/364537/saiba-como-funciona-a-venda-de-dados-pessoais-na-internet. Acesso em: 6 fev. 2024.

Steil, J. Maior vazamento de dados da história expõe brasileiros; veja como checar. *Valor Econômico*, São Paulo, 25 jan. 2024. Empresas. Disponível em: https://valor.globo.com/empresas/noticia/2024/01/25/maior-vazamento-de-dados-da-historia-atinge-brasileiros-veja-como-checar.ghtml. Acesso em: 6 fev. 2024.

Tagiaroli, G. Falha de segurança expõe dados sigilosos em sites do governo. *UOL Tilt*, [*S. l.*], 27 mar. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/03/27/falha-seguranca-sites-do-governo.htm. Acesso em: 19 out. 2024.

Wangham, G.; Santos, P. H.; Moreira, R. Trust and identity: designing an identity solution for digital innovation ecosystems. *In*: XXXIII ISPIM Innovation Conference, Copenhagen, 2022. *Proceedings* [...].Copenhagen, Denmark, 05-08 jun. 2022. Disponível em: https://www.researchgate.net/publication/362074571. Acesso em: 19 out. 2024.

Colaboradores

Conceituação: T. C. P. M. SILVA. Curadoria de dados: B. C. M. NORBIATO e T. C. P. M. SILVA. Análise formal: B. C. M. NORBIATO. Investigação: B. C. M. NORBIATO e T. C. P. M. SILVA. Metodologia: B. C. M. NORBIATO Administração de projetos: T. C. P. M. SILVA. Supervisão: Escrita – rascunho original: B. C. M. NORBIATO e T. C. P. M. SILVA e Escrita – revisão e edição: B. C. M. NORBIATO e T. C. P. M. SILVA.