Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

Autorização judicial para extração de dados em correio eletrônico e redes sociais

Judicial authorization for data extraction in electronic mail and social networks

Ana Luíza Matos de Oliveira[1], Rílary Batista de Lima[2], Agílio Tomaz Marques[3], Barbara Moraes de Mello[4] e Rosana Santos de Almeida[5]

v. 11/ n. 3 (2023)
Julho/Setembro

Aceito para publicação em 15/06/2023.

[1]Graduanda em Direito pela Universidade Federal de Campina Grande;
[2]Graduanda em Direito pela Universidade Federal de Campina Grande;
[3]Doutorando pela Universidade Federal de Campina Grande, Mestre pela Universidade Federal de Campina Grande, Graduado em Direito pela Universidade Federal do Cariri; Juiz de Direito do Tribunal de Justiça da Paraíba;
[4]Mestrando pela Universidade Federal de Campina Grande, Graduado em Direito pela Universidade Federal de Campina Grande; Gerente do Fórum da Comarca de Sousa;
[5]Graduanda em Universidade Federal de Campina Grande.

Resumo: O artigo em questão trata de como a crescente dependência da sociedade em relação às tecnologias digitais têm afetado diretamente na forma em que se apresenta a proteção da privacidade e a necessidade de acesso a esses dados para fins de investigação e aplicação da lei. É abordada a temática da autorização judicial para a extração de dados em correio eletrônico e redes sociais, destacando os fundamentos necessários para a obtenção desse acesso. Apresentando fundamentos jurídicos para tais decisões e tomando como base a Lei de Interceptação Telefônica e o Marco Civil da Internet, assim como estudo de caso prático.

Palavras-chave: Autorização Judicial; Extração de dados; Correio eletrônico; Redes sociais.

Abstract: This article addresses how society's increasing dependence on digital technologies has directly affected the way privacy protection is approached and the need for access to such data for investigation and law enforcement purposes. The theme of judicial authorization for data extraction from email and social media platforms is discussed, highlighting the necessary foundations for obtaining such access. It presents legal foundations for these decisions, drawing on the Law on Telephone Interception and the Internet Civil Rights Framework, as well as case studies.

Keywords: Judicial Authorization; Data extraction; Email, social

1. Introdução

Desde a criação da internet, em meados do século XX, já era possível observar a intenção de alastrar informações de um local a outro. No contexto em que foi criada, a Guerra Fria, é importante observar que seu objetivo era trocar informações de forma mais fácil entre pessoas que estivessem geograficamente distantes, de modo que facilitasse a troca de estratégias de guerra.

Ao continuar em constante evolução, nos últimos anos, o uso generalizado da internet e das redes sociais transformou a forma como as pessoas se comunicam, compartilham informações e interagem socialmente. No entanto, essa crescente dependência das tecnologias digitais também levanta preocupações relacionadas à proteção da privacidade e à necessidade de acesso aos dados armazenados em correio eletrônico e redes sociais para fins de investigação e aplicação

da lei.

A extração de dados em correio eletrônico e redes sociais por autorização judicial é um tema de grande relevância jurídica e social. A necessidade de equilibrar o direito à privacidade individual com a necessidade de garantir a segurança pública e a eficácia da justiça tem gerado debates intensos sobre os fundamentos necessários para a obtenção dessa autorização.

O presente artigo tem como objetivo analisar a dependência criada pelas pessoas às redes, bem como a influência que tais mecanismos têm nos processos judiciais, além dos desafios que são diariamente apresentados ao meio jurídico, principalmente para atestar veracidade do que lhe é apresentado.

Para que seja admitido o uso de algum meio de correio eletrônico ou redes sociais para a extração de dados, é necessário que haja, primeiramente, aval judiciário, o que, se for dado pode ser justificado pelo princípio da proporcionalidade e necessidade.

No meio jurídico, o princípio da proporcionalidade e necessidade é um dos princípios fundamentais aplicados na tomada de decisões judiciais. Esse princípio busca equilibrar a proteção dos direitos individuais com os interesses coletivos ou públicos, garantindo que as medidas adotadas sejam proporcionais e necessárias para atingir um determinado objetivo.

O princípio da proporcionalidade exige que as restrições ou intervenções impostas pelo Estado sejam proporcionais ao objetivo que se pretende alcançar. Isso significa que a medida deve ser adequada, necessária e não deve impor ônus excessivos aos direitos individuais. Em outras palavras, as restrições devem ser apropriadas para resolver o problema em questão e não devem ir além do necessário para atingir tal objetivo.

Esse princípio desempenha um papel crucial na análise da legalidade e constitucionalidade de medidas que envolvem a privacidade e proteção de dados dos usuários.

No caso específico da extração de dados e conversas do WhatsApp, a aplicação do princípio da proporcionalidade e necessidade requer uma avaliação cuidadosa dos interesses em jogo. Por um lado, a investigação e aplicação da lei visam proteger a segurança pública, prevenir atividades criminosas e obter provas relevantes para a justiça. Por outro lado, os direitos à privacidade e proteção de dados são considerados fundamentais e devem ser adequadamente respeitados.

No contexto da legislação e jurisprudência brasileira, o acesso a dados e conversas do WhatsApp sem prévia autorização judicial é considerado ilegal, uma vez que viola o direito à privacidade e à proteção de dados dos usuários. A obtenção dessas informações sem o devido respaldo judicial é considerada uma violação do princípio em questão.

Nos casos em que essa medida for adotada, deve ser adequada para o propósito específico, ou seja, deve haver uma relação direta e relevante entre os dados buscados e a investigação em

andamento. Além disso, a medida deve ser necessária, o que significa que não deve haver alternativas menos invasivas disponíveis para obter as informações desejadas. Se existirem meios igualmente eficazes, mas menos invasivos, eles devem ser preferidos em relação à extração de dados sem autorização judicial.

Portanto, nos casos em que existirem alternativas que estejam protegidas por meios legais onde seja possível extrair as informações necessárias, essas devem ser feitas, de modo que a procura pela extração de dados por meio judicial deve ser feita em último caso.

2. Vida privada e intimidade: Uma questão de Direitos Humanos e Fundamentais

A vida privada e a intimidade são consideradas questões fundamentais de direitos humanos e fundamentais em várias declarações e tratados internacionais. A Declaração Universal dos Direitos Humanos (DUDH), adotada pela Assembleia Geral das Nações Unidas em 1948, estabelece que "Ninguém será objeto de interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem de ataques à sua honra e reputação. Todo o indivíduo tem direito à proteção da lei contra tais interferências ou ataques".

Além disso, o Pacto Internacional sobre Direitos Civis e Políticos (PIDCP), que entrou em vigor em 1976, também protege a vida privada e a intimidade. O artigo 17 do PIDCP estabelece que "Ninguém será sujeito a interferências arbitrárias ou ilegais em sua vida privada, família, lar ou correspondência, nem a ataques ilegais à sua honra e reputação". Esse pacto reconhece a importância de garantir a proteção da vida privada e impede a interferência governamental arbitrária nessas áreas.

Além das declarações e tratados internacionais, muitos países têm suas próprias constituições e leis que protegem a vida privada e a intimidade. Essas proteções podem incluir o direito à privacidade de comunicações, o direito à proteção de informações pessoais, o direito ao segredo bancário, entre outros.

A proteção da vida privada e da intimidade é essencial para preservar a dignidade humana, a liberdade individual e a autonomia. Ela permite que as pessoas controlem as informações pessoais que desejam compartilhar, protege-as contra interferências injustificadas do governo e de terceiros, e assegura que elas possam expressar-se, relacionar-se e desenvolver-se livremente em um ambiente seguro.

No entanto, é importante notar que esses direitos podem ser limitados em certas circunstâncias, como quando há um interesse legítimo e proporcional do Estado, como a proteção da segurança pública ou a prevenção de crimes graves. Essas restrições devem ser estabelecidas por lei e serem necessárias e proporcionais em uma sociedade democrática.

Em resumo, a vida privada e a intimidade são reconhecidas como direitos humanos e fundamentais, protegidos por várias declarações e tratados internacionais, bem como por constituições e leis nacionais. Esses direitos são essenciais para garantir a dignidade e a liberdade individual das pessoas.

3. Conceito de privacidade, intimidade e sigilo

O conceito de privacidade refere-se ao direito de uma pessoa manter suas informações pessoais em segredo e controlar a divulgação e o uso dessas informações por terceiros. É uma condição fundamental para o exercício da liberdade individual e da autonomia.

A privacidade abrange vários aspectos, incluindo a privacidade física, a privacidade de comunicação e a privacidade de dados. A privacidade física diz respeito à inviolabilidade do espaço pessoal de uma pessoa, garantindo que ela possa ter um espaço livre de interferências indesejadas. A privacidade de comunicação refere-se ao direito de se comunicar de forma confidencial, seja por meio de conversas privadas, correspondência ou comunicação eletrônica.

No mundo digital, a privacidade de dados tornou-se um tema especialmente relevante. Ela diz respeito ao controle que os indivíduos têm sobre a coleta, armazenamento, uso e compartilhamento de seus dados pessoais por empresas, organizações governamentais e outras entidades. Isso inclui informações como nome, endereço, número de telefone, histórico de navegação na internet, preferências pessoais e outros dados pessoais sensíveis.

A privacidade é importante para proteger a intimidade, a dignidade e a liberdade de expressão das pessoas. Ela também é fundamental para evitar abusos, discriminação, vigilância excessiva e violações dos direitos individuais. Em muitos países, a privacidade é protegida por leis e regulamentos, e organizações têm a responsabilidade de adotar medidas de segurança adequadas para proteger a privacidade dos indivíduos.

No entanto, é importante observar que o conceito de privacidade está em constante evolução devido ao avanço da tecnologia e das mudanças sociais. O equilíbrio entre privacidade e outros interesses, como segurança pública e inovação tecnológica, é frequentemente debatido e pode variar em diferentes contextos e culturas.

Já a intimidade tem seu conceito relacionado ao de privacidade, mas possuem significados distintos. A intimidade refere-se a uma esfera mais pessoal e emocional da vida de uma pessoa. Está relacionada aos relacionamentos pessoais, emocionais e afetivos que alguém tem com outras pessoas. A intimidade envolve compartilhar experiências, sentimentos, pensamentos e emoções profundas com alguém em um contexto confiável e próximo.

A intimidade pode existir em diferentes tipos de relacionamentos, como amizades íntimas, relacionamentos românticos, laços familiares estreitos, entre outros. Ela envolve um senso de conexão emocional, vulnerabilidade e confiança mútua entre as pessoas envolvidas.

Embora a privacidade esteja mais relacionada ao controle das informações pessoais, a intimidade está mais associada à conexão emocional e ao compartilhamento íntimo com outras pessoas. Embora possa haver sobreposições entre os conceitos em alguns contextos, eles representam aspectos diferentes da vida e das relações humanas.

O sigilo é um conceito que se refere à proteção de informações sensíveis ou confidenciais, garantindo que elas sejam mantidas em segredo e acessíveis apenas a pessoas autorizadas. O sigilo é uma parte importante da segurança da informação e é amplamente aplicado em diversos contextos, incluindo governos, empresas, instituições financeiras, setor de saúde e em muitas outras áreas.

O objetivo principal do sigilo é evitar a divulgação não autorizada de informações que possam causar danos, prejuízos ou violar a privacidade das pessoas. O sigilo é especialmente relevante quando se trata de informações confidenciais, como segredos comerciais, dados pessoais, informações financeiras, estratégias militares, pesquisas científicas, entre outros.

Existem diferentes níveis de sigilo, que variam de acordo com a natureza das informações e o contexto em que estão inseridas. Em alguns casos, a divulgação não autorizada de informações confidenciais pode levar a consequências legais, danos financeiros ou até mesmo riscos à segurança nacional.

Para garantir o sigilo, são adotadas várias medidas de proteção, como criptografia, acesso restrito, autenticação de usuários, protocolos de segurança, treinamento de pessoal, auditorias e outras práticas específicas relacionadas à área de atuação. Além disso, existem leis e regulamentos que estabelecem diretrizes para a proteção de informações confidenciais, como leis de privacidade de dados e segredo de Estado.

Em resumo, o sigilo é o conjunto de medidas e práticas adotadas para garantir a confidencialidade e a proteção de informações sensíveis, evitando sua divulgação não autorizada e preservando a privacidade das pessoas ou a segurança de organizações.

4. A tutela jurídica do Sigilo no Brasil

No Brasil, a proteção constitucional do sigilo é garantida pela Constituição Federal de 1988. O sigilo é considerado um direito fundamental e está previsto em diversos dispositivos constitucionais, que asseguram a sua inviolabilidade em determinadas situações.

O principal fundamento para a proteção do sigilo no Brasil é o direito à intimidade, assegurado

pelo artigo 5º, inciso X, da Constituição. Esse dispositivo estabelece que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização por dano material ou moral decorrente de sua violação.

Além disso, o direito ao sigilo também é protegido em outros dispositivos da Constituição. O artigo 5º, inciso XII, garante o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial, o que é o caso a ser tratado, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

O sigilo também é protegido no âmbito das atividades profissionais e empresariais. O artigo 5º, inciso XIII, da Constituição assegura a inviolabilidade do sigilo da fonte de informações, quando necessário ao exercício profissional, desde que o jornalista não divulgue a identidade da fonte.
É possível fazer uma relação desse conceito de sigilo para com os veículos midiáticos, os correios eletrônicos e as redes sociais.

4. O sigilo como justificativo para a ilegalidade da extração de dados sem autorização prévia judicial

O sigilo constitucional no Brasil NÃO serve como justificativa para a ilegalidade da extração de dados sem autorização prévia judicial. Pelo contrário, a proteção constitucional do sigilo estabelece que a quebra desse sigilo, incluindo a extração de dados, deve ocorrer mediante ordem judicial fundamentada.

Conforme mencionado anteriormente, o artigo 5º, inciso X, da Constituição Federal garante a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. O mesmo artigo, em seu inciso XII, estabelece a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial, para fins de investigação criminal ou instrução processual penal.

Portanto, a extração de dados sem autorização prévia judicial configura uma violação ao direito ao sigilo protegido constitucionalmente. A autorização judicial é necessária para garantir a legalidade da medida, assegurando que ela seja realizada de forma proporcional e de acordo com os princípios constitucionais, como a reserva de jurisdição.

Vale ressaltar que existem leis específicas que regulamentam a quebra do sigilo, como o Código de Processo Penal e a Lei de Interceptação Telefônica. Essas leis estabelecem os requisitos e procedimentos para a obtenção da autorização judicial, bem como as hipóteses em que a quebra do sigilo pode ser justificada.

Em suma, a proteção constitucional do sigilo no Brasil implica que a extração de dados sem

autorização prévia judicial é ilegal. A autorização judicial é essencial para garantir a legalidade e a proteção dos direitos fundamentais, como o direito à intimidade e à privacidade.

5. A ilegalidade da extração de dados na Lei de Interceptação Telefônica

De acordo com a Lei de Interceptação Telefônica, a extração de dados sem autorização prévia judicial é considerada ilegal. A lei estabelece que a interceptação de comunicações telefônicas, inclusive a obtenção de dados, só pode ser realizada mediante ordem judicial, que deve ser fundamentada e especificar a forma de execução da medida.

Além disso, a lei estabelece requisitos específicos para a autorização da interceptação telefônica, como a existência de indícios razoáveis da prática de crime e a necessidade da medida para a investigação criminal. Esses requisitos visam garantir que a quebra do sigilo seja realizada de forma proporcional e justificada, evitando abusos e garantindo a proteção dos direitos fundamentais dos cidadãos.

A Lei de Interceptação Telefônica também prevê a obrigatoriedade de comunicação imediata do juiz responsável pela autorização da interceptação telefônica ao Ministério Público e à autoridade policial. Além disso, determina que as informações obtidas por meio da interceptação devem ser mantidas em sigilo e utilizadas apenas para fins de investigação criminal ou instrução processual penal.

Dessa forma, a referida lei estabelece claramente que a extração de dados sem autorização prévia judicial é ilegal. Visto que a autorização judicial é um requisito essencial para a realização da interceptação telefônica, incluindo a extração de dados, com o objetivo de garantir a legalidade da medida e a proteção dos direitos constitucionais dos indivíduos envolvidos.

6. A ilegalidade da extração de dados no Marco Civil da Internet

No âmbito do Marco Civil da Internet, a extração de dados sem autorização pode ser considerada ilegal, dependendo do contexto e das circunstâncias. A lei estabelece diretrizes específicas para a proteção da privacidade e da segurança dos usuários, bem como para a coleta e o tratamento de dados na internet.

O Marco Civil da Internet estabelece que a coleta, o uso, o armazenamento e o tratamento de dados pessoais devem ser realizados de acordo com o consentimento do titular dos dados ou com base em outras hipóteses previstas na legislação. Além disso, a lei prevê que o provedor de serviços de internet somente poderá disponibilizar informações pessoais do usuário a terceiros mediante

consentimento ou por determinação judicial.

Essas disposições evidenciam que a extração de dados sem o consentimento do titular ou sem uma base legal adequada pode ser considerada ilegal conforme o Marco Civil da Internet. A lei busca garantir a proteção da privacidade dos usuários e estabelece diretrizes claras para o tratamento adequado dos dados na internet.

Ressalta-se que o Marco Civil da Internet também prevê a responsabilidade dos provedores de serviços de internet em relação à guarda e à segurança dos dados dos usuários. Assim, a extração de dados sem as devidas salvaguardas de segurança também pode ser considerada uma violação à legislação.

7. Privacidade e sigilo nos Tribunais

O Supremo Tribunal Federal (STF) mantém posições que divergem na defesa da constitucionalidade quanto à quebra de sigilo das comunicações. Na maioria dos julgados, invoca-se o princípio da razoabilidade e da proporcionalidade. Será utilizado um estudo de caso a partir da base de dados nos sítios de jurisprudência do Supremo Tribunal Federal e Superior Tribunal de Justiça para se compreender a posição de tais tribunais superiores a partir do argumento "privacidade, sigilo de dados, violação". Foram encontrados 14 acórdãos do STF, sendo eles agrupados segundo a identidade dos pedidos envolvidos, e a partir deles foram selecionados 8 mais expressivos que mostram a evolução da jurisprudência sobre o tema para análise individualizada.

A concepção vigente do STF permeia a questão de que os direitos e garantias individuais não têm caráter absoluto e podem ceder em face de outros direitos que são considerados de maior relevância, do interesse social ou público e da justiça, além de situações onde esses direitos e garantias são excepcionais e sirvam de escudo para acobertar condutas consideradas criminosas.

No RE 535.478/SC, de 2008, esse pano de fundo está bem sintetizado, onde a relatora, Min. Ellen Gracie, demonstrou que o tema da proteção aos sigilos bancário e fiscal fora "expressamente abordado pelo STJ no sentido de que o direito à intimidade e privacidade não é direito absoluto, devendo ceder ante à prevalência do direito público sobre o privado, na apuração de fatos delituosos ou na instrução de processos criminais". Posteriori, em 2010, seguiu-se a mesma linha o voto do Ministro Celso de Melo no HC 103.236

> Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto

> constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas - e considerado o substrato ético que as informa - permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros. (MINISTRO CELSO DE MELLO, 2010).

Como observado, existe uma colisão entre a discussão sobre a inexistência de direitos absolutos que recaem em situações excepcionais onde o comportamento das algumas pessoas acaba afetando o comportamento e direitos de outras com o interesse público de manter a paz social, em um sentido amplo, a própria vida comunitária.

Com a intenção de possibilitar maior controle sobre tal componente jurídico, o STF determina que a quebra de sigilo sempre deve ser precedida de respectiva fundamentação para que seja impedido seu uso abusivo e indiscriminado. Segundo o magistério do Ministro Celso de Mello, em voto no HC nº 84.758-GO:

> A quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas, o que daria ao Estado, em desconformidade com os postulados que informam o regime democrático, o poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos alheios. Para que a medida excepcional da quebra de sigilo bancário não se descaracterize em sua finalidade legítima, torna-se imprescindível que o ato estatal que a decrete, além de adequadamente fundamentado, também indique, de modo preciso, dentre outros dados essenciais, os elementos de identificação do correntista (notadamente o número de sua inscrição no CPF) e o lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira. (MINISTRO CELSO DE MELLO, 2010).

Nesse caso em particular há a Lei Complementar n° 105/2001, que é regulada pelo Decreto n° 3.724/2001, que prevê a quebra de sigilo de dados sigilosos e além disso, amplia o acesso a eles para outros órgãos da administração pública. O ponto controverso em relação à lei recai na possibilidade do sigilo de dados ser quebrado a partir de procedimentos da autoridade administrativa sem a autorização judicial. Por conta disso, o STF inicialmente reconheceu a inconstitucionalidade da lei complementar. Em seu voto, o relator Ministro Marco Aurélio entendeu que banaliza a Constituição Federal, a quebra de sigilo sem autorização judicial.

> SIGILO DE DADOS - AFASTAMENTO. Conforme disposto no inciso XII do artigo 5º da Constituição Federal, a regra é a privacidade quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações, ficando a exceção - a quebra do sigilo - submetida ao crivo de órgão equidistante - o Judiciário - e, mesmo assim, para efeito de investigação criminal ou instrução processual penal. SIGILO DE DADOS BANCÁRIOS - RECEITA FEDERAL. Conflita com a Carta da República norma legal atribuindo à Receita Federal - parte na relação jurídico-tributária - o afastamento do sigilo de dados relativos ao contribuinte. (MINISTRO CELSO DE MELLO, 2010).

É notório que o STF foi além dos limites do texto e operou uma modificação constitucional,

na prerrogativa do constituinte derivado.

5. Considerações finais

Ao considerar a questão da extração de dados em correio eletrônico e redes sociais, é fundamental realizar uma análise minuciosa dos direitos individuais à privacidade e dos interesses coletivos envolvidos. Em um mundo cada vez mais digital, em que informações pessoais são compartilhadas e armazenadas em grande escala, torna-se essencial encontrar um equilíbrio entre a proteção da privacidade dos indivíduos e a necessidade de garantir a segurança pública.

Nesse contexto, a obtenção de autorização judicial se mostra um mecanismo crucial para garantir a legalidade e a proporcionalidade das medidas adotadas. Ao requerer a aprovação de um juiz, há um processo de avaliação cuidadosa que leva em consideração os direitos fundamentais dos cidadãos, bem como as circunstâncias e justificativas para a extração dos dados. Isso evita abusos e protege os indivíduos de violações injustificadas de sua privacidade.

É importante ressaltar que a proteção da privacidade, intimidade e sigilo são direitos fundamentais que devem ser preservados em uma sociedade democrática. No entanto, em certas situações excepcionais, como investigações criminais e ameaças à segurança nacional, a coleta de dados pode ser necessária para proteger o bem-estar coletivo. Nesses casos, é fundamental que haja critérios claros e limitações bem definidas para evitar abusos e garantir que as medidas adotadas sejam proporcionais e estritamente necessárias.

Em última análise, o desafio reside em encontrar um equilíbrio adequado entre a proteção dos direitos individuais e a garantia da segurança pública. É necessário que as autoridades competentes estabeleçam políticas e regulamentações claras, baseadas em princípios jurídicos sólidos, que permitam a extração de dados em conformidade com a lei e com respeito aos direitos humanos. A transparência e a prestação de contas são essenciais nesse processo, para que os cidadãos possam confiar que suas informações pessoais estão sendo tratadas de maneira adequada e legal.

Em suma, a extração de dados em correio eletrônico e redes sociais é uma questão complexa que exige uma abordagem cuidadosa e equilibrada. Proteger a privacidade dos indivíduos é fundamental, mas também é necessário garantir a segurança pública em certas circunstâncias. Ao buscar esse equilíbrio, a obtenção de autorização judicial e a definição de limites claros são mecanismos fundamentais para garantir a proteção dos direitos individuais e a legitimidade das ações realizadas.

Referências

BORGES, José Souto Maior. **Princípio da legalidade e da proporcionalidade como limites à discricionariedade administrativa.** Disponível em: https://jus.com.br/artigos/14402/principio-da-legalidade-e-da-proporcionalidade-como-limites-a-discricionariedade-administrativa. Acesso em: 10/06/2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União, Brasília, DF. Acesso em: 13/06/2023

BRASIL. **Decreto nº 3.724, de 2001.** Regulamenta a Lei Complementar nº 105, de 2001, que dispõe sobre o sigilo das operações de instituições financeiras. Diário Oficial da União, Brasília, DF. Acesso em: 13/06/2023

BRASIL. **Lei Complementar nº 105, de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras. Diário Oficial da União, Brasília, DF. Acesso em: 13/06/2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12/06/2023.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal, que trata das interceptações telefônicas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 12/06/2023.

FIGUEIREDO, Marcela Diniz de et al. Privacidade e proteção de dados pessoais no ambiente digital. **Revista de Informação Contábil**, vol. 7, n. 2, 2013. Disponível em: https://www.scielo.br/j/rinc/a/kdqYTvJ7GWsS75twG6f37Bc/. Acesso em: 10/06/2023.

NASCIMENTO, Rafael Rodrigues. **O esvaziamento do princípio da proporcionalidade pelo STF**. Disponível em: https://www.conjur.com.br/2021-set-07/opiniao-esvaziamento-principio-proporcionalidade-stf. Acesso em: 10/06/2023.

SCARDUELLI, **Rodolfo Luiz Viana. Extração de dados e conversas do WhatsApp sem prévia autorização judicial é considerada ilegal.** Disponível em: https://jus.com.br/artigos/54491/extracao-de-dados-e-conversas-do-whatsapp-sem-previa-autorizacao-judicial-e-considerada-ilegal. Acesso em: 10/06/2023.

SUPREMO TRIBUNAL FEDERAL. Habeas Corpus nº 84.758-GO. Relator: Ministro Celso de Mello. Julgado em 2010. Acesso em: 13/06/2023.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário** nº 535.478/SC. Relatora: Ministra Ellen Gracie. Julgado em 2008. Acesso em: 13/06/2023.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário** nº 535.478/SC. Relatora: Ministra Ellen Gracie. Julgado em 2010. Acesso em: 13/06/2023