FACULDADE DOM ADELIO TOMASIN - FADAT
CURSO DE GRADUAÇÃO EM DIREITO

MARIA FERNANDA RODRIGUES DA SILVA

A RECUSA DOS PROVEDORES DE INTERNET EM FORNECER DADOS CADASTRAIS E O CRIME DE DESOBEDIÊNCIA À REQUISIÇÃO DA AUTORIDADE POLICIAL

QUIXADÁ - CEARÁ
2025

MARIA FERNANDA RODRIGUES DA SILVA

A RECUSA DOS PROVEDORES DE INTERNET EM FORNECER DADOS CADASTRAIS E O CRIME DE DESOBEDIÊNCIA À REQUISIÇÃO DA AUTORIDADE POLICIAL

Monografia apresentada como requisito para aprovação na disciplina Trabalho de Conclusão de Curso II e conclusão do Curso de Direito da Faculdade Dom Adelio Tomasin – FADAT.

Professor: Me. André Luis Tabosa de Oliveira

QUIXADÁ - CEARÁ

2025

Dados Internacionais de Catalogação na Publicação (CIP)
FADAT - Educação Superior
Biblioteca Francisca Alexandre Gomes (Dona Mocinha)

SI183

SILVA, MARIA FERNANDA RODRIGUES DA

A RECUSA DOS PROVEDORES DE INTERNET EM FORNECER DADOS CADASTRAIS E O CRIME DE DESOBEDIÊNCIA À REQUISIÇÃO DA AUTORIDADE POLICIAL: / MARIA FERNANDA RODRIGUES DA SILVA. – 2025.

54 f. :

Ilustrações: Não possui.

TCC-Graduação – FADAT - Educação Superior. - Curso de Direito.

Orientação: Mestre(a) ANDRÉ LUIS TABOSA DE OLIVEIRA.

Palavras-chave: CONFLITO, SEGURANÇA PÚBLICA, PRIVACIDADE, DESOBEDIÊNCIA, DADOS.

CDD 740

Gerada automaticamente mediante os dados fornecidos pelo(a) autor(a)

AGRADECIMENTOS

Primeiramente, a Deus, por estar aqui e ter conseguido realizar mais um sonho e por todas estas pessoas que Ele colocou em minha vida.

À minha avó, Francisca, que é o anjo que Deus colocou em meu caminho. Com muito esforço me fez ser quem sou hoje e, mesmo longe geograficamente, se faz presente em minha vida.

À minha mãe, Fabiana, que nos dias de aflição, sua alegria mesmo me questionando o porquê de tudo isso, me contagiava de alguma forma, não me deixando nunca desistir dos meus sonhos. Sua garra me inspirou e suas orações me fizeram chegar aqui.

Ao meu pai, Francisco, que sempre foi meu herói nos momentos difíceis. Sua luta pelos meus sonhos me ensinou a guerrear pela nossa família.

Aos meus irmãos, Eduarda, Emanuele, Adriele, Matheus, Lucas e Moisés, que, em momentos difíceis dessa jornada, conseguiram mostrar a essência da vida com cada risada proporcionada. Cada um à sua maneira, me alcançando de formas únicas.

Aos meus tios, Flaviana e André, que sempre fizeram mais do que serem tios, foram como pais para mim, apoiando-me em tudo.

Aos meus avôs, Vera, João, Francisco, Gerardo, Emanuel, que desde muito cedo, me ensinaram sobre batalhas e a importância de nunca desistir, pois no fim, o esforço vale a pena, o trabalho edifica o homem.

Ao meu orientador, Mestre André, que sempre me compreendeu de forma singular, buscando me acalmar nos momentos mais difíceis. Seu cuidado e atenção me motivaram a chegar aqui. É uma referência para mim, não poderia haver pessoa melhor para guiar-me nessa jornada árdua, mas recompensadora.

Aos meus amigos, que carrego no peito, que torcem por mim, mesmo à distância. Aqueles que me ajudaram da forma que puderam, com conversas, com envios referentes a este trabalho, ou simplesmente me tirando um pouco do mundo acadêmico para aliviar a mente.

A todos os professores do Curso de Bacharelado em Direito da FADAT, pelo conhecimento, pela motivação e pela amizade.

Aos meus colegas de turma e da faculdade, pela parceria, companheirismo e união em todos os momentos.

À FADAT, por todo apoio e dedicação face aos universitários.

“Teu dever é lutar pelo Direito, mas no dia em que encontrares em conflito o Direito e a Justiça, luta pela justiça.”

(Eduardo Juan Couture)

PÁGINA DE APROVAÇÃO

A RECUSA DOS PROVEDORES DE INTERNET EM FORNECER DADOS CADASTRAIS E O CRIME DE DESOBEDIÊNCIA À REQUISIÇÃO DA AUTORIDADE POLICIAL

MARIA FERNANDA RODRIGUES DA SILVA

Trabalho de Conclusão de Curso - Monografia - apresentado à Banca Examinadora e aprovado em 23/06/2025.

_____

Prof. Orientador

_____

Prof. Trabalho de Conclusão de Curso II

_____

1º Avaliador

_____

2º Avaliador

DECLARAÇÃO DE ISENÇÃO DE RESPONSABILIDADE

A Faculdade Dom Adelio Tomasin - FADAT, na representação do Curso de Direito e de seus docentes, declara isenção de responsabilidade por produções incompatíveis com as normas metodológicas e científicas, bem como por obras com similaridades parciais, totais ou conceituais, sendo de responsabilidade dos alunos a produção e a qualidade das mesmas, bem como a veracidade, a verossimilhança e a confiabilidade dos dados apresentados nos trabalhos.

gov.br
Documento assinado digitalmente
MARIA FERNANDA RODRIGUES DA SILVA
Data: 08/07/2025 17:38:52-0300
Verifique em https://validar.iti.gov.br

Acadêmico

RESUMO

A presente monografia analisa o conflito jurídico entre o direito à privacidade dos usuários de internet e a necessidade de acesso a dados cadastrais em investigações criminais. Com o avanço das tecnologias digitais, a internet tornou-se uma ferramenta essencial para a vida moderna, mas também um ambiente propício à prática de crimes. Nesse contexto, os dados pessoais passaram a ter elevado valor estratégico, exigindo regulamentação específica para sua proteção. Assim, surgiram o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), estabelecendo princípios e deveres para o uso responsável da informação digital. O trabalho destaca que, embora a Constituição Federal de 1988 assegure a inviolabilidade da intimidade e do sigilo de dados, esses direitos não são absolutos e podem ser relativizados em prol do interesse público, especialmente na seara investigativa. A autora analisa a legalidade das requisições de dados cadastrais por autoridades policiais sem ordem judicial, com base no artigo 10, §3º, do Marco Civil, e discute a possibilidade de configuração do crime de desobediência diante da recusa injustificada por parte dos provedores. A pesquisa demonstra a lacuna legislativa quanto à delimitação exata de quais dados podem ser requisitados, apontando riscos à privacidade e à segurança jurídica. Por fim, defende-se a necessidade de equilíbrio entre a eficácia da persecução penal e a proteção dos direitos fundamentais, por meio de interpretações normativas cautelosas e atuação responsável dos agentes públicos e privados envolvidos.

Palavras-chave: Conflito. Segurança Pública. Privacidade. Dados. Proteção. Investigação Criminal. Desobediência.

ABSTRACT

This monograph analyzes the legal conflict between the right to privacy of internet users and the need for access to registration data in criminal investigations. With the advancement of digital technologies, the internet has become an essential tool for modern life, but also a fertile ground for the commission of crimes. In this context, personal data has gained significant strategic value, requiring specific regulation for its protection. Thus, the Civil Rights Framework for the Internet (Marco Civil da Internet) and the General Data Protection Law (LGPD) were enacted, establishing principles and duties for the responsible use of digital information. The study highlights that, although the 1988 Federal Constitution guarantees the inviolability of privacy and data confidentiality, these rights are not absolute and may be relativized in favor of public interest, especially in the context of criminal investigations. The author examines the legality of requests for registration data by police authorities without prior judicial authorization, based on Article 10, §3 of the Civil Rights Framework, and discusses the possibility of characterizing the crime of disobedience in cases of unjustified refusal by internet providers. The research demonstrates a legislative gap regarding the exact definition of which data may be requested, pointing out risks to privacy and legal security. Finally, the study advocates for the need to balance the effectiveness of criminal prosecution with the protection of fundamental rights, through cautious legal interpretations and responsible conduct by both public and private actors involved.

Keywords: Conflict. Public Security. Privacy. Data. Protection. Criminal Investigation. Disobedience.

SUMÁRIO

1 INTRODUÇÃO

A sociedade passa por constante evolução, dentre elas o uso da *internet* é evidente em todos os indivíduos, desse modo, há uma grande interação entre pessoas de diferentes locais, fazendo com que informações sejam bombardeadas o tempo todo, mostrando, portanto que a ferramenta *internet* possui suas vantagens e desvantagens.

Conforme a interação foi se intensificando, o processamento de dados também, haja vista que quanto mais pessoas usando a *internet*, mais dados são processados, ademais, a *internet* proporciona ampla facilidade em diversas áreas, permitindo, por exemplo, a assinatura de documentos, contratos e operações financeiras de forma totalmente digital, resultando em maior praticidade e agilidade nas relações cotidianas. Diante desse avanço, tornou-se indispensável a criação de uma legislação específica para regulamentar o tratamento de dados pessoais, considerando os riscos associados ao seu uso indevido, como vazamentos de informações, fraudes e a prática de crimes mediante o acesso não autorizado a esses dados.

Essa coleta escalonada ensejou um cenário propício ao cometimento de crimes, considerando que houve grande aumento de risco de lesão a privacidade e do sigilo de informações, os quais são direitos previstos na Constituição Federal de 1988 (CF/88).

Assim, como cada área do Direito resguarda algum bem, a exemplo o Direito do Consumidor resguardando as relações consumeristas, o Direito das Famílias amparando as relações de contrato, viu-se a necessidade de uma legislação para proteção dos usuários. Com isso, se deu o surgimento da Lei Geral de Proteção de Dados (LGPD), bem como o Marco Civil da Internet e o Decreto que regulamenta o mesmo, logo, com o avanço tecnológico surgiu um novo mundo dentro da sociedade, requerendo essas novas regras, ainda que, os crimes cometidos fossem parecidos com os consumados no mundo físico. A exemplo o *bullying*, com a criação do mundo virtual, ensenjou o *cyberbullying*, a modalidade do crime em ambiente online.

Contudo, a *internet* teve seu avanço, mas não se limitando apenas a situações que prejudicam seus usuários, no âmbito das investigações criminais, essa ferramenta tem sido um grande aliado para identificação de possíveis criminosos, desse modo, em contrapartida, como supracitado, apesar de ser uma situação visando a proteção da coletividade, que também são usuários, por outro lado, há outros usuários com seus direitos violados, em detrimento da segurança pública.

Outrossim, apesar de haver legislações específicas não há uma delimitação assertiva acerca do que seria autorizado fornecer em caso de requisições e se esse tipo de diligência precisaria de fato de uma ordem judicial, como não há demarcação, acaba que tanto as

autoridades quanto os provedores, podem fazer mais do que devem, podendo acontecer o fornecimento ou a requisição de dados que não cabem compartilhamento, por se enquadrarem em outra espécie de dados, logo, violando direitos do indivíduo, gerando abusos.

Portanto, as requisições são procedimentos administrativos de suma importância para cumprir com os princípios da Administração Pública, sendo essencialmente a celeridade e eficiência, os quais são amparados pela constituição, o que significa que caso não seja cumprido por alguma situação, consequentemente tal circunstância é punível.

Pois ao passo que se busca garantir a proteção dos dados pessoais dos usuários, a não observância das requisições formuladas por autoridades policiais pode comprometer o andamento de investigações criminais, dificultando a responsabilização dos agentes envolvidos. Essa problemática suscita a necessidade de se refletir sobre a existência de um ponto de equilíbrio entre a tutela da privacidade e a efetividade da atuação dos órgãos responsáveis pela segurança pública.

Diante do exposto, a presente temática mostra-se relevante para a elucidação de casos concretos no contexto abordado, exigindo a análise crítica das argumentações apresentadas pelas partes envolvidas, notadamente autoridades policiais e provedores de *internet*, bem como a apreciação dos fundamentos jurídicos que sustentam suas posições. Ao final, busca-se identificar qual entendimento deve prevalecer, em conformidade com a jurisprudência firmada pelo Supremo Tribunal Federal, visando à solução equilibrada do conflito em questão.

Desse modo, acerca do contexto supramencionado, o presente trabalho se delimita nesse tipo de caso concreto, em que a problemática se concentra na possibilidade de enquadrar os provedores de internet no crime de desobediência, bem como se a requisição de dados cadastrais feita por autoridade policial necessita de ordem judicial, traçando objetivos acerca das consequências dessa recusa dos provedores, bem como em que se baseam para tal ato negativo, de modo a analisar também a harmonia entre as normas conflitantes. Desse modo, a metodologia utilizada fora a abordagem qualitativa de caráter exploratório e teórico, análise comparativa entre legislações e o entendimento dos Tribunais.

Na pesquisa há menção quanto aos agentes, procedimentos dos dados, provedores, bem como, a responsabilidade desse último e afins. Não obstante, há grande explanação sobre o embate de direitos envolvido no cenário, esses, previstos na CF/88, dado que, é o centro da discussão atual. Por fim, o entendimento dos Tribunais acerca da discussão buscando harmonizar as normas, para que não aja conflitos.

2 OS PROVEDORES DE INTERNET E A GUARDA DE DADOS CADASTRAIS

Os provedores de internet têm um papel fundamental no uso e distribuição da *internet* em todo o mundo. Muitas vezes, quando se fala em *internet*, a maioria dos indivíduos imagina diretamente os sites, as redes sociais ou até aplicativos, como se fossem a origem de tudo, no entanto, antes de qualquer acesso, estão os provedores, os responsáveis por viabilizar a conexão e permitir que as informações circulem no ambiente virtual. Além de fornecer o acesso, esses provedores também possuem importantes responsabilidades, especialmente no que se refere à guarda dos dados cadastrais de seus usuários.

2.1 O direito fundamental à privacidade e a internet: aspectos gerais dos dados cadastrais

A priori, sabe-se que a Constituição Federal de 1988 é a Carta Magna do ordenamento jurídico brasileiro, responsável por prever os direitos e garantias fundamentais. Dentre o que é assegurado no rol do art. 5, destaca-se a privacidade, sua proteção está diretamente vinculada ao princípio da dignidade da pessoa humana, além disso, com os avanços tecnológicos e a ampla circulação de informações no ambiente digital, o bem da privacidade ganha ainda mais relevância. Por conseguinte, o artigo supramencionado conceitua privacidade como:

> 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:
> […]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> […]
> 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;

Com isso, o inciso X e XII, respectivamente, protege uma esfera individual pessoal de cada indivíduo, enquanto o outro traz a proteção no campo das comunicações, garantindo que o sigilo de correspondência, das comunicações e afins é inviolável, mas às suas exceções. A CF busca equilibrar a proteção dos direitos individuais em comparação dos direitos coletivos. Embora cada direito busque algo como a segurança pública ou a proteção dos direitos fundamentais, como a privacidade e a dignidade, é necessário haver uma harmonia nessa busca.

2.1.1 Paralelo Entre Privacidade e Constituição Federal

Diante disso, é possível traçar um paralelo para melhor entendimento sobre a privacidade e sua não absolutização, utilizando como exemplo o direito à vida, esse, embora seja um direito fundamental e esteja expressamente protegido pela Constituição Federal de 1988, também não é considerado absoluto. Isso significa que, em determinadas situações, ele pode ceder diante de outros direitos ou circunstâncias excepcionais. Um exemplo que ilustra isso é a legítima defesa, que configura uma excludente de ilicitude no âmbito penal. Nessa situação, mesmo que tirar a vida de alguém, em regra, seja considerado um crime tipificado no Código Penal, em seu art. 121, a legislação entende que, se essa ação ocorre para proteger a própria vida ou a de terceiros, não há ilicitude.

Portanto, o direito penal reconhece que, em casos extremos, preservar a própria integridade física pode justificar até mesmo um ato que, em outro contexto, seria um crime grave. Esse entendimento demonstra que, embora extremamente relevante, a vida não é protegida irrestritamente em todas as circunstâncias, pois o contexto faz toda a diferença, é uma forma de reconhecer que às vezes, a necessidade de proteger a própria vida pode sobrepor a vida de quem representa uma ameaça.

Da mesma forma, a privacidade, também classificada como um direito fundamental, previsto no art. 5 da Constituição Federal de 1988, não possui caráter absoluto no ordenamento jurídico brasileiro. Isso significa que, em determinadas situações, ela pode ser relativizada, especialmente quando entra em conflito com outros direitos igualmente relevantes ou interesses coletivos, como o presente tema, em investigações criminais, é possível haver quebra de sigilo telefônico, bancário ou de dados, desde que autorizada judicialmente e com fundamentação adequada, com sua real motivação.

Com isso, busca-se garantir a efetividade da justiça e o combate à criminalidade, ademais, situações que envolvem segurança pública, defesa nacional ou proteção de terceiros podem justificar a mitigação desse direito. Nesse contexto, se estabelece um necessário equilíbrio entre a proteção da privacidade individual e o interesse coletivo na preservação da ordem pública.

2.1.2 Da ponderação de princípios

A privacidade, enquanto direito fundamental, não é absoluto, como supramencionado, no entanto, qualquer restrição deve observar critérios de legalidade, necessidade,

proporcionalidade e razoabilidade, para evitar abusos e assegurar que a intervenção estatal ocorra somente nos estritos limites dos interesses públicos. Assim, o desafio contemporâneo reside em harmonizar esses dois pilares.

Assim, é evidente que tanto a vida quanto a privacidade estão inseridas em um contexto de ponderação de valores e princípios, no qual o equilíbrio entre direitos é essencial para a harmonização da convivência em sociedade e para a própria manutenção do Estado Democrático de Direito, pois viver em sociedade exige que às vezes alguns interesses individuais sejam limitados em favor de um bem comum. Por conseguinte, os direitos supramencionados demonstram que, na prática, nenhum direito é totalmente intocável, ao haver de se basear pelo contexto e suas necessidades.

2.1.3 Aspectos Dados Cadastrais

Dessa forma, é necessário fazer alguns parâmetros a fim de evitar os abusos e buscar o equilíbrio entre a privacidade individual e a segurança coletiva, quando há investigações criminais esses direitos entram em conflito. Tendo em vista a busca pela harmonização entre esses direitos, a Lei Geral de Proteção de Dados, traz uma gama de conceitos acerca dos diversos tipos de dados, no presente contexto, trata-se da limitação do que seria dado cadastral ou pessoal, como está previsto na LGPD, a seguir:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Desse modo, segundo a LGPD, dizendo respeito a informações relacionadas a pessoa, como exemplo, nome, idade, filiação e afins, pois através deles é possível identificar determinado indivíduo, além de disporem também sobre gostos e personalidade de determinada pessoa. A exemplo do conceito, se baseando em dados com os registros expostos a seguir, transmitirão uma informação sobre alguém.

Com base nestes registros: (I) Jogadora de futebol mundialmente conhecida, (II) Eleita diversas vezes a melhor do mundo, (III) É atleta da seleção brasileira. Diante dessas informações é possível que muitas pessoas já identificariam que esses dados correlacionados transmitem a informação acerca de quem seja esse indivíduo, de modo a se tratar da jogadora Marta, contudo, com somente dois dados algumas pessoas já assimilariam o resultado da informação.

Conforme o exemplo exposto, Bruno Bioni (2019) conceitua dados da seguinte forma:

> O dado é o estado primitivo da informação, pois não é nada, que, por assim dizer, acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação.

Ainda, partilha do mesmo entendimento Soler (2021):

> Em poucas palavras, dado pessoal pode ser um nome, um endereço, até placa do carro, restaurante favorito, link da rede social, tamanho da roupa, etc.19, bastando a sua devida contextualização, organização, tratamento e/ou interpretação para que ele, ao trazer um significado ou mesmo ter algum sentido, transformar-se em informação.

Desse modo, há grande conflito entre os doutrinadores quanto ao limite do que seria dado pessoal, embora, a legislação traga sua disposição não delimita de fato o que seria, fazendo com que empresas ou até mesmo autoridades cometam equívocos quanto a requisição.

2.1.4 Dados sensíveis

Adiante, tem-se também o conceito de dados sensíveis. Esses dizem respeito a características de cunho mais íntimo, elementos que para se ter ciência somente uma pessoa próxima a esse indivíduo teria acesso, de modo que, com o acesso a esses elementos por indivíduos mal-intencionados pode causar danos, lesá-los de forma mais grave, pois com algum referido elemento, o indivíduo pode divulgar, fazendo com que possivelmente a vítima sofra algum tipo de discriminação, pois esse tipo de registro dispões acerca de etnia, religião, pensamento político, saúde, vida sexual, orientação sexual e afins.

No tratamento de dados sensíveis a LGPD é muito rigorosa, pois nela há aceitação de tratamento desses dados em duas situações com seus devidos procedimentos. A primeira hipótese é com o consentimento do titular, sendo esse, claro, livre, específico e explícito, e claro, havendo uma motivação, uma finalidade previamente informada para tal ato, com isso, o indivíduo deve ser ciente tanto de quais dados serão acessados, quanto a finalidade para esse acesso.

A segunda, diz respeito quando não se tem o consentimento do titular, e nessa segunda hipótese a lei é bem mais rigorosa, mas permite o tratamento dessas informações ainda assim, de modo que, é necessária uma determinação legal, para realização de pesquisas, porém, garantindo a confidencialidade, para a garantia do exercício regular do direito, há também a possibilidade como método de prevenção, bem como, para proteger a vida ou a integridade

física do titular, ou de terceiros, nesse último, poderia correlacionar-se nos casos de investigações criminais.

Essa rigorosidade serve para os dados sensíveis serem tratados de forma responsável, requerendo ética, transparência, segurança, e somente sejam processados dados haver necessidade para atingir sua finalidade, buscando a minimização do uso de dados, coletando o que for realmente necessário, visando a proteção a privacidade dos indivíduos, com a garantia da confidencialidade, bem como, adotar medidas que impeçam vazamento desses dados, além de acessos não autorizados, para que assim não seja colocado em risco a privacidade e os direitos do titular das informações.

Diante do exposto, embora os dados sensíveis sejam algo mais íntimo para os indivíduos, os dados cadastrais também são submetidos aos mesmos cuidados, o que difere é somente a finalidade desses tipos de informações e a maior facilidade em acessá-los.

2.2 A lei geral de proteção de dados e o tratamento de dados cadastrais

O surgimento da LGPD no Brasil, ocorreu com o avanço da tecnologia e das redes, haja vista que nesse ambiente há uma grande interação entre os usuários, seja essa troca de forma direta ou indireta, assim como cada ramo do direito resguarda algum bem, a exemplo o Direito Civil protegendo as relações de contratos, famílias, o Direito do Consumidor com sua proteção acerca das relações consumeristas, sendo cada área responsável pela proteção de algum direito. Desse modo, o Direito Digital vem para proteger a privacidade e a liberdade dos usuários no Brasil.

Conforme mencionado por Renato Leite Monteiro (2018), em demais países existe a mesma preocupação, a exemplo do GDPR (General Data Protection Regulation), que regulamenta a questão no âmbito da União Europeia. A LGPD, porém, vai além do GDPR, expandindo o escopo da proteção de dados. Sendo assim, o surgimento da LGPD não ocorreu de uma forma isolada, fora fortemente influenciado por um movimento global de fortalecimento da proteção de dados. Nesse contexto, refere-se ao Regulamento Geral de Proteção de Dados da União Europeia, tornando referência mundial na área voltada a proteção de dados.

Nesse sentido, a LGPD dispõe de diversos conceitos acerca da privacidade de usuários, quais sejam: titular, tratamento de dados, dados pessoais, dados pessoais sensíveis, dados anonimizados, anonimização, consentimento, agentes de tratamento, encarregado e transferência internacional de dados, todos esses elementos constroem a base de segurança

para processamento de dados, prezando pela responsabilidade e privacidade.

2.2.1 Elementos conceituais

Desse modo, respectivamente significa, titular refere-se, ao proprietário dos dados a serem tratados, sendo sempre uma pessoa física, natural, identificada ou identificável, a quem se referem os dados pessoais. A proteção conferida ao titular é um dos pilares da LGPD, visando assegurar sua privacidade, adiante, o tratamento de dados dispõe acerca de toda e qualquer operação realizada com dados pessoais, independente do meio, do país de sua sede ou do local onde estejam os dados, isso tudo ampara um conjunto de ações, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração.

2.2.2 Diferença entre dado pessoal e anonimizado

Além disso, no quesito dados pessoais em sua definição é compreendida a toda e qualquer informação relacionada a uma pessoa identificada ou identificável, como o nome, sobrenome, apelido, idade, filiação, informações essas que permitem identificar um indivíduo, esses podem ser isolados, ou os dados podem ser combinados, para que correlacionados identifiquem alguém. No mesmo sentido há também os dados pessoais sensíveis, aqueles que estão relacionados a personalidade e escolhas dos indivíduos, dispondo acerca da religião, opinião política, orientação sexual e afins, é um conteúdo sensível, pois se vazado poderá lesar aquele titular por poder haver discriminação e coisas do gênero.

Prosseguindo, os dados anonimizados são o oposto dos dados pessoais, apesar de tratarem de um titular dessas informações, ocorre que, esses dados não podem identificar alguém seja de forma direta ou indireta, considerando a utilização de meios técnicos razoáveis e disponíveis para tal tratamento dessas informações. Essa anonimização consiste em um processo pelo qual os dados pessoais a serem tratados são submetidos a técnicas que desvinculam qualquer conexão com a identificação do titular.

Desse modo, o dado pessoal, posteriormente, anonimizado deixará de ser considerado um dado pessoal para fins da aplicação da LGPD, pois se entende que aquele dado deixou de ser um risco a privacidade do usuário. Com isso, o dado anonimizado poderá ser utilizado para diversas finalidades caso seja garantido que não haja sua reversão quanto a reidentificação da pessoa.

2.2.3 Agentes de Tratamento

Já os agentes de tratamento estão compreendidos em 3 pessoas, quais sejam: controlador, operador e encarregado, respectivamente são: pessoa natural ou jurídica que recepciona os dados pessoais dos titulares por meio do consentimento como supracitado, ou por hipótese de exceção, esse é o principal responsável para que tudo ocorra conforme a LGPD; este diz respeito a pessoa que realiza o tratamento dos dados por contrato ou obrigação legal; por fim, é a pessoa indicada pelo controlador, porém a LGPD previu que tanto o controlador como o operador poderiam indicar, mas que atribuiu o dever somente ao controlador, atuando assim como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Quanto a transferência internacional de dados, diz respeito quando há o envio ou disponibilização de dados pessoais para país estrangeiro, ou para organismo internacional do qual o Brasil seja membro, de modo que, isso inclui situações em que os dados são armazenados em servidores localizados fora do país, acessados por empresas estrangeiras. A LGPD dispõe que para essa transferência ocorrer, deverá ser assegurada as condições que garantem um nível de proteção adequado e compatível com o previsto na legislação brasileira. Com isso, o país destinatário dos dados precisa oferecer as garantias de proteção à privacidade, segurança e direitos dos titulares, como exposto no art. 33 da LGPD:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

No mesmo sentido disserta ainda Ruth Maria Guerreiro (2022):

> Para que os dados pessoais sejam tutelados pela LGPD não são levados em consideração: o país sede da empresa, o meio de operação e tratamento de dados, a localização dos dados e nem mesmo a nacionalidade do titular dos dados, bastando que se encontre em território nacional no momento da coleta.

Com isso, entende que o compartilhamento de dados é algo cada vez mais evidente, no cotidiano ou mesmo para outros fins específicos, há uma maior facilidade para alcançar as finalidades do processamento desses dados, e isso se dá em esfera internacional.

2.2.4 Atividades de Tratamento

Progredindo, sabendo a gama de artigos da LGPD amparando essas situações, é importante ressaltar que a lei não é composta e analisada somente com base nos artigos

dispostos, mas são regidos também por uma série de princípios, os quais estão inseridos no art. 6 da LGPD sem seus 10 (dez) incisos, quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, detalhados a seguir.

De causas a efeitos, a finalidade, refere-se para qual fim aquele dado será tratado, de modo que, esse princípio dispõe que dados pessoais só podem ser coletados para um objetivo claro e determinado, que deverá ser comunicado ao titular, para que assim expresse sua ciência, ou seja, toda coleta de dados requer uma motivação. Quando se fala em adequação, seguindo a mesma linha da finalidade, serão tratados somente dados pertinentes e coerentes para atingir o propósito que justificou a coleta desses, a exemplo, indivíduo A forneceu seus dados para participar de um curso da empresa B, ocorre que esses dados coletados não podem ser usados para algum tipo de campanhas de marketing que não estejam vinculadas a esse curso sem seu devido consentimento.

A necessidade, é o princípio responsável por limitar o tratamento ao mínimo necessário para atingir aquele fim pretendido, desse modo, os dados coletados devem partir do princípio de evitá-los, somente coletar os imprescindíveis, pois qualquer tipo de informação que puder ser evitada, será, a exemplo, indivíduo A no momento de fazer um cadastro numa loja, o estabelecimento solicita alguns dados pessoais, de modo a não fazer sentido a solicitação sobre informações acerca da religião ou orientação sexual.

Quanto ao livre acesso é garantido que o titular tenha acesso fácil e gratuito aos dados que estão em processo de tratamento, bem como informações sobre o processo, esse acesso vai do que está sendo armazenado a para quem será compartilhado.

Sob a ótica de Tarcísio Teixeira (2022) sobre o tratamento e transparência de dados, ressalta:

> Para cada finalidade será colhido um consentimento específico, sendo que o titular consente a utilização de seus dados pessoais para um propósito informado previamente, atendendo-se ao princípio da transparência.

Dessa forma, o princípio da transparência assegura ao titular dos dados maior segurança quanto ao uso de suas informações pessoais, promovendo um ambiente de confiança e previsibilidade. Isso porque é essencial que o indivíduo tenha pleno conhecimento sobre as razões que justificam a coleta e o tratamento de seus dados, bem como sobre as finalidades específicas a que se destinam. Tal conhecimento deve ser contínuo e atualizado, acompanhando o fluxo do tratamento, de modo que o titular possa, a qualquer momento, compreender como, por que e por quem suas informações estão sendo utilizadas.

2.2.5 Direitos dos titulares dos dados

Assim como supramencionado acerca do surgimento do GDPR, trouxe uma série de mudanças referente a privacidade, além de estabelecer deveres para com empresas, provedores de internet e entre outros, introduziu também os direitos dos titulares de dados a serem tratados, esses, são um conjunto de garantias estabelecidas pela LGPD, como também supracitado influenciado pelo GDPR. Os titulares, indivíduos que tenham seus dados coletados ou tratados, ganharam um maior controle sobre o uso e finalidade de suas informações, quais sejam: acesso, correção e exclusão.

A LGPD é muito conexa em seus princípios, direitos, deveres e artigos, quando disposto sobre o direito ao acesso, relaciona-se com transparência, clareza e finalidade, ao ser resguardado que o titular saberá quais dados estão sendo utilizados além do porquê e como essas informações serão tratadas, a motivação para aquela diligência, e a exemplo desse direito se pode citar quando um indivíduo solicita cópia de seus dados que determinada empresa possui.

No mesmo sentido, o Direito a correção garante que o titular corrija ou atualize suas informações cadastrais, caso sejam imprecisas, desatualizadas e até mesmo incompleta, isso serve para evitar possíveis transtornos para com o titular, como decisões equivocadas com base em dados errados, essas alterações deverão ser realizadas de imediato e sem demora, especialmente se afetarem decisões importantes. Contudo, caso seja reconhecido pela organização que a alteração é inválida, se fundada em erro ou algo do tipo, deverá ser apresentada uma explicação ao titular.

Por fim, a exclusão, também conhecido como “direito ao esquecimento”, esse permite que o indivíduo solicite a eliminação de seus dados pessoais em processo de tratamento pela organização, essa medida visa garantir que dados não permaneçam por mais tempo que o necessário, além de assegurar o titular que ele tem poder sobre seus dados, podendo solicitar exclusão quando quiser, todavia, se houver alguma justificativa legal, algum tipo de contrato ou obrigação que justifique o mantimento dessas informações, elas não poderão ser removidas. Além disso, havendo solicitada a remoção sem nenhum impedimento, se esses dados são compartilhados entre entes terceiros, a remoção deverá ser comunicada a essas também.

2.2.6 A ANPD e sua função

Ainda que o tratamento de dados pessoais envolva diversas etapas e requisitos legais, existe um órgão especificamente incumbido de zelar pela observância e fiscalização da norma: a Autoridade Nacional de Proteção de Dados (ANPD).

Dessa forma, o tratamento de dados pessoais demanda a observância rigorosa de uma série de princípios e cuidados estabelecidos pela Lei Geral de Proteção de Dados, cuja aplicação é supervisionada pela Autoridade Nacional de Proteção de Dados (ANPD). Em um cenário onde a informação se consolida como um ativo estratégico de altíssimo valor, torna-se essencial a adoção de mecanismos rígidos de controle e proteção, a fim de garantir a preservação da privacidade dos titulares e mitigar eventuais violações a seus direitos fundamentais.

2.3 O Marco Civil da Internet e a Responsabilidade dos Provedores de Internet

Assim como a LGPD, o Marco Civil da Internet surgiu com o propósito de regulamentar as relações no ambiente digital, especificamente no âmbito da *internet*. Essa legislação estabelece os princípios, garantias, direitos e deveres para o uso da internet no Brasil, funcionando como um marco normativo para assegurar direitos dos usuários e responsabilidades dos provedores de internet, haja vista que, um novo mundo requer novas regras, e assim aconteceu com o avanço da internet.

2.3.1 A LGPD e o Marco Civil da Internet

Diferentemente da LGPD, que possui um foco específico na proteção de dados pessoais e na privacidade dos usuários, o Marco Civil tem uma abrangência mais ampla, disciplinando as bases para o uso da internet de forma geral. Enquanto o Marco Civil se dedica a garantir a liberdade de expressão, aos direitos fundamentais no ambiente virtual e a privacidade no ambiente digital, a LGPD aprofunda-se nos procedimentos, obrigações, direitos e deveres relacionados ao tratamento dos dados pessoais, promovendo a segurança e o respeito à privacidade.

Embora, as duas legislações atuem em campos correlacionados, não se revogam por coexistirem, muito menos há uma sobreposição, ao contrário, possuem uma relação de complementariedade, ao fortalecerem mutuamente na construção de um ambiente digital mais

seguro, transparente e ordenado pela proteção dos direitos fundamentais de cada usuário.

Nesse sentido, a LGPD dita as regras em situações específicas, expondo conceitos sobre dados, agentes, tratamento de dados e uma série de procedimentos, dentro ou fora da internet. Enquanto, o Marco Civil da Internet dispõe de forma geral sobre o uso da internet, em um sentido amplo, porém, restrito no que diz respeito ao ambiente de uso.

Com isso, a finalidade dessa lei é a garantia do uso da internet de forma livre, segura, democrática, participativa e responsável, assegurando a proteção dos direitos fundamentais no ambiente digital, para que se promova a liberdade de expressão, a inviolabilidade das comunicações, a proteção da privacidade com o grande auxílio da LGPD.

À primeira vista, quando se pensa sobre LGPD ou Marco Civil da Internet alguns indivíduos remetem isso a tecnologia, ambiente online e afins, contudo, a origem desse contexto são os provedores de internet, esses são empresas ou organizações que fornecem o acesso, serviços na rede mundial de computadores: a internet. Eles atuam como intermediários para a internet chegar ao usuário final, permitindo que pessoas físicas e jurídicas possam se conectar, acessar conteúdos e utilizar dos serviços online.

Observa-se que os provedores de acesso à internet detêm um vasto conjunto de informações relativas aos seus usuários, incluindo dados cadastrais, registros de conexão e, em alguns casos, de navegação. Embora essa assimetria informacional possa, à primeira vista, sugerir uma relação de vulnerabilidade do usuário em face do provedor, em analogia ao vínculo de hipossuficiência existente nas relações trabalhistas, é imprescindível destacar que essas empresas estão submetidas a um arcabouço normativo rigoroso.

2.3.2 Da responsabilidade e suas hipóteses

Dessa forma, impõem-se aos provedores de serviços obrigações legais específicas relativas à guarda, ao tratamento e à proteção dos dados pessoais dos usuários. A inobservância desses deveres, seja por conduta dolosa, negligente ou pelo uso indevido das informações, poderá acarretar a responsabilização civil do provedor. Tal responsabilização encontra amparo nos princípios fundamentais da legislação aplicável, notadamente os da boa-fé, da finalidade, da segurança da informação e da prestação de contas, conforme estabelecido pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados Pessoais.

Com isso, quando se fala em responsabilidade, atualmente no ordenamento jurídico possuem duas teorias que englobam a responsabilidade civil, essas se diferenciam no quesito da imprescindibilidade da culpa, para que assim haja a obrigação de reparar o dano, sendo

estas, subjetiva e objetiva.

Nesse contexto, a responsabilidade subjetiva exige, como requisito essencial, a demonstração do elemento culpa, seja na modalidade de dolo ou negligência, imprudência ou imperícia, para haver a imputação da obrigação de indenizar. Ausente a culpa, inexiste responsabilidade. Por outro lado, na responsabilidade objetiva, a obrigação de reparar o dano independe da comprovação de culpa, sendo fundamentada na teoria do risco, segundo a qual aquele que exerce determinada atividade assume os riscos a ela inerentes, devendo responder pelos prejuízos causados, ainda que de forma involuntária.

2.3.3 Espécies de Provedores

Desse modo, para maior clareza é necessária uma distinção entre os tipos de provedores existentes, que a junção deles faz com que a internet alcance o mundo. Com isso, destacam-se entre suas espécies os provedores *backbone*, provedores de acesso, de correio eletrônico, de hospedagem, de conteúdo, de conexão e de aplicação.

O *Backbone*, ou espinha dorsal da rede, constitui o mais elevado grau hierárquico da estrutura de uma rede de computadores, sendo responsável pelo transporte da maior parte dos dados que circulam na internet. Trata-se de uma infraestrutura física de alta capacidade, geralmente composta por cabos de fibra óptica de grande velocidade e desempenho, capaz de sustentar o tráfego intenso e contínuo de informações em âmbito global.

Nesse contexto, o provedor de *backbone* é a pessoa jurídica que detém e opera tais estruturas técnicas, sendo titular de redes compostas por roteadores de alto desempenho interligados por circuitos de transmissão de dados em alta velocidade. Esses recursos são, em regra, disponibilizados a terceiros como provedores de acesso à internet e empresas de hospedagem de dados mediante contraprestação pecuniária. Tal relação evidencia a relevância estratégica do provedor de *backbone* para a manutenção e funcionamento adequado da rede mundial de computadores no território nacional, constituindo elemento essencial à infraestrutura da informação no Brasil.

Já o provedor de acesso são agentes exercem função essencial na cadeia de comunicação digital, uma vez que possibilitam o ingresso dos usuários na internet por meio de infraestrutura tecnológica própria ou mediante conexão contratada junto a um *backbone*. Em ambos os casos, cabe a esses provedores garantir a estabilidade, a disponibilidade e a segurança da conexão ofertada, elementos que impactam diretamente na experiência do usuário e na efetividade dos serviços digitais.

Ato contínuo, o provedor de hospedagem consiste na pessoa jurídica responsável por disponibilizar espaço em servidores de sua propriedade para o armazenamento remoto de dados, permitindo que terceiros acessem essas informações conforme as condições previamente ajustadas com o contratante do serviço. Além da hospedagem de conteúdo digital, tais empresas frequentemente oferecem serviços complementares, como o registro de nomes de domínio, a realização de *backups* periódicos do conteúdo hospedado e outras funcionalidades voltadas à segurança e à manutenção do site.

Ainda, quanto ao provedor de conteúdo, é definido como a pessoa natural ou jurídica que disponibiliza informações, textos, imagens, vídeos ou quaisquer dados na internet, sendo, em regra, o responsável direto pela criação, produção ou curadoria desse material. Sua atuação consiste em tornar acessível ao público determinado conteúdo informativo ou comunicacional, utilizando para isso servidores próprios ou os serviços de um provedor de hospedagem.

Ademais, o provedor de conexão é a pessoa jurídica responsável por viabilizar o acesso dos usuários à internet, por meio da oferta de serviços que permitem a conexão entre os terminais e a rede mundial de computadores. No contexto brasileiro, destacam-se como exemplos de provedores de conexão as empresas de telecomunicações como TIM, Claro e Vivo.

2.3.4 Da distinção entre a situação de responsabilidade civil e penal por parte dos provedores

A responsabilidade civil dos provedores, nesse cenário, se fundamenta no dever jurídico de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A falha nesse dever revela não somente negligência, mas também um desequilíbrio entre os interesses econômicos da empresa e os direitos fundamentais do titular de dados.

Por outro lado, a questão da requisição de dados cadastrais por autoridades policiais ou pelo Ministério Público levanta importantes discussões quanto à legalidade, aos limites e às consequências do não atendimento a essas requisições. Conforme dispõe o art. 13-B do Código de Processo Penal e o §3º do art. 10 do Marco Civil da Internet, essas autoridades podem requisitar diretamente determinados dados cadastrais, sem necessidade de autorização judicial prévia, desde que observadas as finalidades legais e os princípios da necessidade e da proporcionalidade.

No entanto, é preciso cautela quanto à natureza dessas requisições. A doutrina e parte da jurisprudência apontam para a necessidade de se delimitar claramente o tipo de dado requisitado, sob pena de desvio de finalidade e violação da intimidade do titular. Ainda, há controvérsia quanto à qualificação jurídica da requisição como ordem legal: para que sua desobediência configure o crime previsto no art. 330 do CP, é imprescindível que a ordem emanada por autoridade competente esteja revestida de legalidade, clareza e pertinência ao caso concreto.

2.3.5 Guarda de registros e o seu vínculo com a requisição

No que tange às obrigações atribuídas aos provedores de conexão à internet, merece destaque o disposto no artigo 13 do Marco Civil da Internet (Lei nº 12.965/2014), o qual estabelece a obrigatoriedade da guarda dos registros de conexão. Tais registros constituem elemento essencial para a efetivação de eventuais requisições por parte das autoridades competentes. Conforme o referido dispositivo legal, os provedores devem manter esses dados pelo prazo de 1 (um) ano, em ambiente seguro, controlado e de acesso restrito, visando assegurar a integridade, confidencialidade e disponibilidade das informações.

Importante ressaltar que essa obrigação é de natureza exclusiva dos próprios provedores de conexão, sendo-lhes vedada a transferência ou delegação da responsabilidade de guarda dos registros a terceiros. Essa vedação reforça o compromisso legal desses agentes com a segurança e rastreabilidade dos dados, constituindo mecanismo fundamental para subsidiar investigações e preservar direitos fundamentais no ambiente digital.

Dessa forma, decorrido o prazo legal de guarda estipulado pelo Marco Civil da Internet, os provedores de conexão ficam autorizados a proceder à exclusão dos registros de conexão, segundo a legislação vigente. Essa determinação encontra respaldo também na Resolução n.º 614, de 28 de maio de 2013, da Agência Nacional de Telecomunicações (Anatel), que igualmente estabelece o prazo de um ano para a conservação de tais registros.

2.3.6 Descumprimento da guarda de registros

Cumpre salientar que o descumprimento dessa obrigação legal por parte dos provedores poderá ensejar a aplicação de sanções de natureza judicial e administrativa, em razão da omissão quanto à manutenção das informações exigidas por lei. Tais medidas visam garantir a efetividade da investigação de ilícitos no ambiente digital e a preservação de

direitos fundamentais, ao mesmo tempo, em que impõem aos provedores um dever rigoroso de diligência no tratamento dos dados sob sua responsabilidade.

> Art. 53. A Prestadora deve manter os dados cadastrais e os Registros de Conexão de seus Assinantes pelo prazo mínimo de um ano.
> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Portanto, é notório que os provedores de internet integram um papel importante acerca dos dados coletados, ao armazenarem as informações temporariamente para fins de possíveis uso daquele dado.

2.3.7 Distinção entre dados cadastrais, conexão e conteúdo

Com a devida distinção entre dados cadastrais, dados de conexão e dados de conteúdo, observa-se uma significativa diferenciação entre essas categorias. Tal distinção, prevista especialmente no Marco Civil da Internet, pretende modular o grau de proteção conferido a cada tipo de dado, considerando o nível de sensibilidade e a exposição do titular. Contudo, apesar de sua clareza teórica, essa diferenciação revela vulnerabilidades práticas, lacunas normativas e potenciais riscos à efetiva proteção dos direitos fundamentais.

Os dados cadastrais, por conterem informações básicas de identificação, foram colocados pelo legislador sob um regime de menor proteção jurídica, autorizando seu acesso sem ordem judicial, conforme o art. 10, §3º do Marco Civil da Internet. Essa exceção, embora justificada sob a ótica da celeridade investigativa, enfraquece o controle jurisdicional sobre o uso de dados pessoais, podendo abrir margem para abusos e requisições genéricas por parte das autoridades.

Na prática, o vago conceito de “dados cadastrais” gera incertezas, pois informações como endereço IP ou localização, embora técnicos, podem ser utilizados para identificar padrões comportamentais. A ausência de um rol taxativo sobre o que são dados cadastrais compromete a segurança jurídica e fere o princípio da legalidade estrita, essencial no campo das restrições de direitos fundamentais.

Embora classificados como dados técnicos, os dados de conexão possuem alto potencial de identificação, especialmente quando combinados com outros elementos, como IP e porta lógica. Por isso, o legislador foi mais cauteloso ao condicionar o acesso a esses registros à autorização judicial, conforme exigido pelo art. 10, §2º do Marco Civil da Internet.

Todavia, na prática, há dificuldade operacional e técnica na guarda e fornecimento

desses dados por parte dos provedores, além de desafios relacionados à correta identificação da porta lógica e à precisão dos registros. Essa limitação tecnológica pode afetar a eficácia das investigações criminais, especialmente em crimes praticados no ambiente virtual.

Os dados de conteúdo representam o nível mais profundo e sensível de informação, por revelarem aspectos subjetivos da intimidade do usuário. Por isso, o acesso a esses dados é restrito à autorização judicial e fundamentado no princípio do sigilo das comunicações, consagrado no art. 5º, XII da Constituição Federal.

Nesse aspecto, o ordenamento jurídico brasileiro está em conformidade com os padrões internacionais de proteção de dados. No entanto, a proteção constitucional não elimina os riscos de violação por parte do próprio Estado ou agentes privados, o que evidencia a necessidade de mecanismos eficazes de fiscalização, rastreabilidade das requisições e responsabilização em caso de abuso.

2.3.8 Natureza da requisição dos dados cadastrais

Já no quesito da natureza da requisição de dados realizada por autoridades policiais ou pelo Ministério Público tem natureza jurídica de ato administrativo vinculante, cujo objetivo é coletar informações necessárias para a investigação criminal e atividades correlatas. Diferentemente de uma ordem judicial, essa requisição, em regra, não exige autorização prévia do Judiciário para ser emitida, embora deva respeitar os limites estabelecidos pela legislação e pela Constituição.

Essa medida decorre do poder conferido a essas autoridades para conduzir investigações, conforme previsto em dispositivos legais, como os artigos 13-A e 13-B do CPP e o artigo 10, §3º do Marco Civil da Internet. Todavia, para que essa requisição seja legítima, é imprescindível que observe princípios fundamentais, incluindo legalidade, proporcionalidade e respeito à privacidade dos indivíduos.

3 O CRIME DE DESOBEDIÊNCIA À REQUISIÇÃO DA AUTORIDADE POLICIAL DE DADOS CADASTRAIS

A presente seção aborda o crime de desobediência relacionado ao não atendimento, sem justificativa, da requisição de dados cadastrais feita pela autoridade policial. Trata-se de uma medida que visa garantir a efetividade da investigação criminal, assegurando o acesso célere a informações básicas, como nome, filiação e endereço, sem a necessidade de autorização judicial. A análise deste delito se mostra relevante diante dos desafios impostos pela proteção de dados pessoais e pela busca do equilíbrio entre o dever de colaboração com o Estado e os direitos fundamentais dos indivíduos. Neste contexto, serão examinados os elementos caracterizadores do crime e seus fundamentos legais.

3.1 A Requisição de dados cadastrais pela autoridade policial: contexto legal

Em um cenário cada vez mais avançado como o do Brasil, em que antes o cometimento de crimes eram ocorridos somente no âmbito físico, com o surgimento da internet “novos crimes” foram surgindo também, entre aspas porque, apesar de serem cometido em um novo mundo, grande parte deles, são crimes do mundo físico aplicado ao ambiente virtual, por isso a existência do cyberbullying, que consiste no bullying em ambiente virtual, a vista disso, muitos crimes foram superlotando o país, crimes esses que a população questionava se a internet era de fato uma “terra sem lei”, e com essa valoração, passou a legislar.

Todavia, esse mundo não veio só trazer coisas prejudiciais, ocorre que em muitos procedimentos investigativos, há uma necessidade de saber mais sobre aquele indivíduo, ora investigado, como hoje quase todas as pessoas têm acesso à internet, seus dados estão a todo momento sendo processados e guardados, visando sua proteção.

Desse modo, a legislação brasileira permite que a autoridade policial requisite dados cadastrais diretamente para fins investigativos, sem a necessidade de prévia autorização judicial. Entretanto, essa prerrogativa não está isenta de controvérsias, uma vez que envolve o equilíbrio entre dois valores fundamentais: de um lado, o interesse público na repressão e investigação de ilícitos penais; de outro, os direitos fundamentais à intimidade, privacidade e proteção dos dados pessoais, assegurados pela Constituição Federal.

3.1.1 Procedimento da requisição

Ato contínuo, quando a autoridade policial busca esse tipo de informação, é necessário ir ao ponto de origem, requisitar aos provedores de internet, ao serem o ponto de acesso de todos os usuários, bem como guardam informações numa espécie de nuvem de armazenamento. A requisição de dados cadastrais pela autoridade policial enquadra-se das medidas investigativas, visando a celeridade para resolução de casos, bem como, a segurança pública, no ordenamento jurídico brasileiro essa diligência encontra respaldo na LGPD e no Marco Civil da Internet, de modo a buscar equilibrar os interesses nesse tipo de situação, pois de um lado se tem o Estado garantidor da segurança da coletividade, enquanto do outro tem um particular, um investigado com seus dados a serem processados.

O ponto de partida para qualquer análise sobre a obtenção de dados pessoais por agentes estatais reside na própria Constituição Federal de 1988, que assegura, no artigo 5º, inciso X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo o direito à indenização pelo dano material ou moral decorrente de sua violação. Além disso, o inciso XII protege o sigilo das comunicações telefônicas, de dados e de correspondências, ressalvando as hipóteses e formas legais de quebra de sigilo, mediante ordem judicial.

No que se refere ao Código de Processo Penal (CPP), embora este não disponha expressamente sobre a requisição de dados cadastrais, é possível interpretar, com base em suas normas gerais sobre a investigação criminal, que cabe à autoridade policial a prática de todos os atos necessários à apuração da infração penal, desde que respeitados os direitos e garantias fundamentais do investigado. Essa compreensão decorre do poder e dever de investigar atribuído à polícia judiciária, notadamente nos termos dos arts. 6º, inciso III, e 13 do CPP, que autorizam a colheita de elementos probatórios e a requisição de informações essenciais à elucidação do fato criminoso.

Ainda no âmbito do CPP, os artigos 13-A e 13-B tratam da requisição de informações por autoridades investigativas, autorizando, em termos específicos, que a autoridade policial ou o Ministério Público requeiram dados de vítimas, ou investigados diretamente de empresas prestadoras de serviços de telecomunicações e tecnologia da informação. No entanto, esses dispositivos restringem essa prerrogativa a determinados crimes, previstos nos artigos 148, 149, 149-A, § 3º do artigo 158 e artigo 159 do Código Penal Brasileiro, ou seja, crimes como sequestro, cárcere privado, trabalho análogo ao de escravo, extorsão mediante sequestro e crimes correlatos.

Esses delitos têm em comum a violação à liberdade individual, razão pela qual o legislador conferiu tratamento excepcional para permitir requisições diretas, sem necessidade de autorização judicial prévia, visando proteger a integridade da vítima em situações de urgência., todavia, mesmo diante da limitação legal expressa quanto ao tipo penal, é possível sustentar, sob a ótica dos princípios constitucionais da proporcionalidade, da razoabilidade e da eficiência da persecução penal, uma interpretação sistemática e finalística desses dispositivos. Isso significa que, em casos concretos que envolvam risco à vida, à dignidade da pessoa humana ou à ordem pública, pode se admitir, em caráter excepcional e justificado, a extensão da requisição direta de dados, especialmente se houver respaldo em outros dispositivos legais como o art. 13 do CPP ou o art. 10, §3º do Marco Civil da Internet, sendo estes:

> Art. 13-A. Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei no 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos.
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> [...]
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

Tal interpretação deve sempre ser orientada pela ponderação entre direitos fundamentais, como a privacidade e a intimidade do titular dos dados e a necessidade de apuração criminal eficaz, evitando excesso e garantindo que os princípios do devido processo legal e da legalidade estrita sejam respeitados, buscando harmonizar as normas e adaptando-as ao caso concreto, para dirimir quaisquer incoerências jurídicas.

Com isso, a principal finalidade da requisição de dados cadastrais é viabilizar a pronta identificação e localização de vítimas, suspeitos ou testemunhas em emergências, esse tipo de medida é geralmente adotado nas fases iniciais da investigação criminal, quando a autoridade policial precisa de respostas rápidas para direcionar diligências, evitar o desaparecimento de provas ou salvar uma vida em risco. Assim, o mecanismo garantirá maior efetividade na atuação policial e permitir ações preventivas e investigativas imediatas, preservando, dentro do possível, os direitos fundamentais dos envolvidos.

A requisição de dados cadastrais diretamente pela autoridade policial é uma ferramenta legítima e necessária para a efetividade da investigação criminal no Brasil,

especialmente nos casos mais graves, como supramencionado, contudo, essa prerrogativa não pode ser utilizada abusivamente, devendo ser proporcional, fundamentada e limitada aos dados estritamente necessários. O equilíbrio entre a eficiência investigativa e a proteção dos direitos fundamentais, especialmente a privacidade, deve ser constantemente observado, com atenção às normas da LGPD, do Marco Civil da Internet e da própria Constituição Federal. A atuação transparente e responsável das autoridades é essencial para assegurar a legalidade e a legitimidade desse tipo de medida no Estado Democrático de Direito.

Tal diligência encontra respaldo legal no Marco Civil da Internet, especificamente em seu artigo 10, §3º, o qual autoriza, expressamente, a requisição de dados cadastrais por autoridades policiais ou pelo Ministério Público, independentemente de prévia autorização judicial. No entanto, tal previsão tem sido objeto de intensa controvérsia doutrinária, uma vez que parte da doutrina entende que o dispositivo representa uma lacuna técnica ou equívoco legislativo, ao permitir o acesso direto a informações pessoais sem o devido controle jurisdicional. Ainda assim, a interpretação literal do dispositivo confere suporte normativo para tais requisições diretas.

Conforme analisado, o artigo 10, §3º, do Marco Civil da Internet estabelece uma exceção à regra de proteção dos dados pessoais, ao permitir que autoridades policiais e o Ministério Público tenham acesso direto a dados cadastrais sem a necessidade de autorização judicial prévia. No entanto, essa disposição tem sido objeto de intensos debates doutrinários, especialmente quanto à imprecisão normativa.

Segundo doutrinadores, George Leite e Ronaldo Lemos (2014), entendem que:

> Cumpre observar, no entanto, a exceção prescrita no § 3o do artigo 10 da Lei no 12.965, no qual estipula que, excepcionalmente, é facultado o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. O referido § 3o, no entanto, não estipula quais seriam as "autoridades administrativas" que seriam competentes para a requisição dos dados cadastrais. Sobre o assunto, no Senado Federal, a Emenda no 20 ao então PLC 21/2014 (denominação de quando o Marco Civil tramitou na Casa como Projeto de Lei) buscava esclarecer quais seriam essas autoridades, passando a contemplar expressamente no artigo que seriam o Delegado de Polícia e os membros do Ministério Público. O texto vigente da Lei, contudo, foi aprovado no Senado sem que fosse incluída qualquer das Emendas, tendo restado a referida lacuna. Buscando a ratio legis e a occasio legis do Marco Civil, é possível extrair que, efeti- vamente, quis o legislador referir a que os Delegados de Polícia e os membros do Mi- nistério Público são as autoridades competentes para tal solicitação, em consonância com o já mencionado artigo 15 da Lei no 12.850/2013, a qual trata das organizações criminosas.

O dispositivo não explicita com clareza quais dados específicos se enquadram na categoria de "dados cadastrais", o que pode gerar interpretações amplas e, consequentemente, abusos na requisição por parte das autoridades. A ausência de limitação expressa quanto ao

tipo de dado a ser fornecido contribui para o receio de que a norma possa servir como porta de entrada para violações à privacidade e à proteção de dados, contrariando os princípios constitucionais e os ditames da própria Lei Geral de Proteção de Dados.

Além disso, ao estabelecer essa exceção à exigência de ordem judicial, o §3º acaba por relativizar a tutela da privacidade, que, em regra, exige o crivo do Judiciário para mitigação. Tal prerrogativa concedida às autoridades administrativas, sem a devida regulamentação e controle, revela um tensionamento entre o interesse público na persecução penal e os direitos fundamentais do cidadão.

> O § 3o do art. 10 traz uma exceção à regra de que o fornecimento de registros só se dará por meio de ordem judicial. O acesso a dados cadastrais, por autoridades administrativas que detenham competência legal para requi- sição dos dados, não dependerá, logicamente, de autori- zação judicial. Para parte da doutrina especializada sobre o tema, o Marco Civil teve falha grave, em não especificar (detalhar) o que é dado pessoal (cadastral) e sua diferença em relação a dado ou registro de conexão, em relação ao assinante. Analisando-se o Marco Civil, percebe-se que, para obtenção dos dados de conexão ou de acesso a aplicações (que incluem o endereço IP), exige-se ordem judicial. Já de posse do IP, com base no § 3o do art. 10, as autoridades administrativas (p. ex., Polícia, Ministério Público, CADE, Anatel, CGU, Receita Federal, Abin, dentre outras) pode- riam requerer os dados cadastrais associados, em tese, sem ordem judicial. Uma falha no Marco Civil da Internet. Destaca-se que muitos especialistas criticaram este ponto, sobretudo diante da ausência de ampla discussão no Congresso Nacional. Releva notar que dados de conexão ou de acesso a aplicações (com o fornecimento de IPs) não identificam, em um primeiro momento, um usuário. Já, por sua vez, os dados cadastrais qualificam e identificam o usuário. Outra corrente doutrinária, ainda, entende que o § 3o do art. 10 do Marco Civil apenas consigna que este não Destaca-se que muitos especialistas criticaram este ponto, sobretudo diante da ausência de ampla discussão no Congresso Nacional. Releva notar que dados de conexão ou de acesso a aplicações (com o fornecimento de IPs) não identificam, em um primeiro momento, um usuário. Já, por sua vez, os dados cadastrais qualificam e identificam o usuário. Outra corrente doutrinária, ainda, entende que o § 3o do art. 10 do Marco Civil apenas consigna que este não revoga os arts. 17-B da Lei n. 9.613/98 (com redação dada pela Lei n. 12.983/2012, “para tornar mais eficiente a per- secução penal dos crimes de lavagem de dinheiro”) e 15 da Lei n. 12.850/2013, já em vigor.

Dessa forma, embora o artigo 10, §3º, possua respaldo legal, carece de maior rigor técnico e normativo, razão pela qual parte da doutrina o considera incompleto e potencialmente lesivo aos direitos fundamentais, clamando por uma interpretação restritiva ou mesmo por uma futura revisão legislativa que melhor delimite o seu alcance e aplicação.

3.1.2 Do Protocolo de Internet e da Porta Lógica

Ademais, o Marco Civil da Internet contempla elementos relativos aos chamados registros de conexão, os quais compreendem, entre outros, a data e hora de início e término de uma conexão à internet, além do endereço de Protocolo de Internet (IP) utilizado. A controvérsia doutrinária se intensifica justamente nesse ponto, uma vez que, embora o artigo

10, §3º da referida norma autorize a requisição de dados cadastrais sem ordem judicial, o IP que permite identificar o local de acesso à rede – extrapolaria essa categoria, por representar elemento mais sensível, próximo dos chamados dados de rastreamento.

Nesse cenário, os críticos sustentam que o IP não pode ser equiparado a dado meramente cadastral, pois, por sua natureza técnica, possibilita a localização geográfica aproximada do usuário, o que, na prática, representa uma ingerência na esfera da intimidade e da privacidade, exigindo, portanto, autorização judicial prévia.

Outro aspecto relevante está na relação entre o IP e a porta lógica de origem. Para fins de analogia didática, pode-se afirmar que o IP funcionaria como o número de um edifício, enquanto a porta lógica equivaleria ao número de um apartamento dentro desse edifício. Assim, a porta lógica permite uma identificação mais precisa do terminal utilizado em determinada conexão, sendo essencial para a correta individualização do usuário, especialmente em redes com IP compartilhado, como ocorre comumente em ambientes corporativos e residenciais.

Portanto, a identificação do IP isoladamente pode ser insuficiente, sendo necessária também a indicação da porta lógica para garantir a exatidão da informação, reforçando a necessidade de criteriosa delimitação legal sobre o alcance dos dados que podem ser requisitados extrajudicialmente pelas autoridades.

Entretanto, o Superior Tribunal de Justiça (STJ) já firmou entendimento, por meio de voto da relatora Ministra Nancy Andrighi, no sentido de que o provedor de conexão à internet tem o dever de identificar os usuários de seus serviços com base no endereço IP utilizado e no período aproximado do acesso em que teria ocorrido o suposto ato ilícito, não sendo necessária, para tanto, a indicação prévia da porta lógica de origem pelo requerente. O entendimento estabelece que a ausência desse dado técnico específico não exime o provedor da obrigação legal de colaborar com a identificação do usuário, nos moldes do disposto no Marco Civil da Internet, conforme ementa a seguir:

> RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. E-MAIL DIFAMATÓRIO. IDENTIFICAÇÃO DE USUÁRIO. PROVEDOR DE CONEXÃO. NEGATIVA DE PRESTAÇÃO JURISDICIONAL. AUSÊNCIA. IDENTIFICAÇÃO DE IP SEM PORTA LÓGICA. OBRIGAÇÃO DO PROVEDOR. INTERVALO DE 10 (DEZ) MINUTOS. POSSIBILIDADE.
>
> 1. Ação de obrigação de fazer ajuizada em 2/8/2023, da qual foi extraído o presente recurso especial, interposto em 7/6/2024 e concluso ao gabinete em 17/9/2024.
>
> 2. O propósito recursal é decidir se o provedor de conexão deve individualizar o usuário diante de (i) identificação do IP, sem a informação de porta lógica; e (ii) período que compreende intervalo de 10 (dez) minutos.
>
> 3. Não há ofensa aos arts. 489 e 1.022 do CPC quando o Tribunal de origem

> examina, de forma fundamentada, a questão submetida à apreciação judicial e na medida necessária para o deslinde da controvérsia, ainda que em sentido contrário à pretensão da parte.
>
> 4. A jurisprudência desta Corte Superior firmou-se no sentido de que tanto provedores de aplicação quanto provedores de conexão têm a obrigação de guardar e fornecer as informações relacionadas à porta lógica de origem.
>
> 5. Não há necessidade de prévia informação por parte do provedor de aplicação sobre a porta lógica para que o provedor de conexão disponibilize os demais dados de identificação do usuário, pois também esse segundo agente está obrigado a armazenar e fornecer o IP (e, portanto, a porta lógica).
>
> 6. Na requisição judicial de disponibilização de registros (art. 10, §1º, Marco Civil da Internet), para identificação de usuário, não há necessidade de especificação do minuto exato de ocorrência do ilícito.
>
> 7. No recurso sob julgamento, (i) não há necessidade de acionar a provedora de aplicação para informar a porta lógica, pois é dado que a própria recorrente deve possuir; e (ii) inexiste prejuízo à proteção de dados na indicação de período que compreende 10 (dez) minutos.
>
> 8. Recurso especial conhecido em parte e desprovido.

Desse modo, é perceptível que essa requisição e o deferimento do julgado por parte do STJ implica o fator eficiência e celeridade por parte da administração pública, pois, fornecer o que já se tem sendo requisitado é mais importante do que todo um aparato para melhor localização e identificação.

3.2 O Crime de Desobediência no Direito Penal Brasileiro

O crime de desobediência está previsto no art. 330 do CP, o qual integra um rol de crimes contra a Administração Pública e o bem jurídico tutelado a eficiência, a autoridade e o regular funcionamento das atividades administrativas do Estado, com isso, tem como sujeito ativo e passivo, respectivamente: qualquer indivíduo pode ser sujeito ativo desse delito, desde que não seja funcionário público, pois nesse caso configuraria crime funcional próprio. Já no contexto de requisição de dados, costuma ser sujeito ativo em potencial do crime caso descumpra a ordem legal de fornecimento de informações, o responsável pela empresa, geralmente o representante legal, o diretor jurídico, ou o encarregado de dados.

Assim partilha conceitua Cléber Masson (2025):

> O núcleo do tipo é “desobedecer”, no sentido de desatender ou recusar cumprimento à ordem legal de funcionário público competente para emiti-la. Não há emprego de grave ameaça ou de violência à pessoa do agente público ou de outra pessoa qualquer, sob pena de desclassificação para o crime de resistência (CP, art. 329). O sujeito, passivamente, limita-se a infringir o mandamento do representante do Poder Público.

Conforme exposto, para ocorrer o crime de desobediência é imprescindível que a ordem tenha sido emanada por agente público competente e esteja revestida de legalidade. Em outras palavras, exige-se que a ordem seja legítima, ou seja, fundamentada em lei e proferida nos limites da atribuição funcional do agente público, assim tipifica o código penal, conforme exposição a seguir "Art. 330 - Desobedecer a ordem legal de funcionário público: Pena - detenção, de quinze dias a seis meses, e multa."

Assim, eventual ordem proferida por autoridade incompetente ou desprovida de respaldo legal não possui força coercitiva suficiente para ensejar a prática do delito, haja vista tratar-se de comando inválido, afastando a tipicidade penal da conduta. Logo, o art. 330 do CP ao prever a punição do descumprimento de ordem legal de funcionário público, o referido dispositivo não se refere a qualquer ordem genérica, mas sim àquela que esteja revestida dos requisitos indispensáveis.

Ressalta ainda, Cezar Bittencourt (2024):

> A conduta incriminada consiste em desobedecer ordem legal de funcionário público, que significa descumprir, desobedecer, desatender dita ordem. É necessário que se trate de ordem, e não de mero pedido ou solicitação, e que essa ordem dirija-se expressamente a quem tenha o dever jurídico de obedecê-la; deve, outrossim, a ordem revestir-se de legalidade formal e substancial. Ademais, "o expedidor ou executor da ordem há de ser funcionário público, mas este, na espécie, entende-se aquele que o é no sentido estrito do direito administrativo", como pontificava Nélson Hungria262. Em outras palavras, a ordem deve emanar de funcionário competente para emiti-la; não sendo funcionário competente, não se poderá falar em crime, por carecer de legalidade em seu aspecto formal.

Ainda no que se refere à competência do agente público para a emissão da ordem (elemento indispensável à configuração do crime de desobediência) é fundamental compreender que a mera aparência de autoridade não legitima o exercício de atribuições que extrapolem a esfera de competência legal do agente. Em outras palavras, para que a ordem seja válida e, consequentemente, passível de gerar a responsabilização penal em caso de descumprimento, é imprescindível que a autoridade esteja devidamente investida na função pública e atue nos estritos limites de sua competência legal.

Assim, a ordem deve ser emanada por agente público autorizado, no exercício regular de suas atribuições e revestida de legalidade. A ausência de qualquer desses requisitos, seja a legalidade da ordem, seja a competência do agente torna o comando inválido, afastando a tipicidade penal da conduta do particular.

No cotidiano jurídico e social, diversos agentes públicos exercem competências específicas decorrentes de suas atribuições legais, sendo, portanto, responsáveis pela emissão

de ordens cuja inobservância pode, em determinadas circunstâncias, configurar o crime de desobediência. Por exemplo, o policial possui a atribuição legal de realizar a prisão em flagrante, sempre que presentes os requisitos legais. Os agentes de trânsito, por sua vez, detêm competência para autuar condutores e aplicar sanções administrativas, como multas, diante de infrações previstas no Código de Trânsito Brasileiro.

Já o magistrado, no exercício de sua função jurisdicional, tem autoridade para determinar a prisão cautelar de indivíduos, bem como aplicar sanções em casos de obstrução à atividade jurisdicional. Um exemplo disso ocorre quando uma pessoa regularmente sorteada para compor o conselho de sentença como jurado no Tribunal do Júri deixa de comparecer injustificadamente, hipótese em que o juiz poderá impor multa, conforme previsão legal. Esses exemplos ilustram como diferentes agentes públicos exercem poderes específicos cuja desobediência, se ilegalmente rejeitada pelo particular, pode ensejar responsabilização penal.

3.2.1 Dos elementos do crime de desobediência

No que se refere ao requisito da legalidade, é imprescindível que a ordem emanada da autoridade pública esteja devidamente respaldada no ordenamento jurídico, conforme já exposto. A legalidade constitui pressuposto essencial para a configuração do crime de desobediência, razão pela qual, mesmo que a ordem seja proferida por agente competente, se for contrária à lei ou violadora de direitos fundamentais, não poderá gerar efeitos jurídicos válidos nem ensejar responsabilização penal.

A ordem será considerada ilegal, portanto, nas seguintes hipóteses: quando violar preceitos constitucionais, especialmente os direitos e garantias fundamentais; quando contrariar disposição legal expressa; ou ainda quando for proferida por agente público que, embora regularmente investido em cargo público, exceda os limites de sua competência funcional ao emiti-la. Nessas circunstâncias, a conduta do particular em não a cumprir, não poderá ser caracterizada como desobediência penalmente punível, diante da ausência de tipicidade.

Dessa forma, diante da emissão de uma ordem considerada ilegal, é facultado ao particular questioná-la, alegando sua invalidade perante a autoridade judicial competente. Caberá, então, ao Poder Judiciário a análise do caso concreto, observando os elementos de legalidade, competência e finalidade do ato administrativo, a fim de verificar se a ordem reúne os requisitos necessários à sua validade.

Ressalte-se que a verificação da legalidade é elemento essencial para aferir a

tipicidade da conduta no âmbito do crime de desobediência, sendo indispensável que a ordem descumprida esteja plenamente conforme o ordenamento jurídico para que se configure o ilícito penal. Portanto, a atuação judicial é imprescindível nesse contexto, a fim de evitar que o cidadão seja responsabilizado por descumprir ordem manifestamente ilegítima.

Prosseguindo, observa-se que o crime de desobediência pode se manifestar sob diferentes formas, sendo insuficiente, para sua configuração, a mera inércia ou omissão por parte do agente. É necessário haver uma conduta voluntária e consciente, que revele a intenção deliberada de descumprir a ordem legalmente emanada por autoridade competente.

Tal conduta pode se expressar de maneira explícita, por meio de negativa verbal, ou ainda por resistência passiva, caso evidencie o dolo. Importa salientar que a simples impossibilidade fática de cumprimento da ordem, desde que devidamente justificada, não configura o delito em comento, uma vez que inexiste, nesse caso, a voluntariedade necessária à caracterização da tipicidade penal.

Como partilha o entendimento os doutrinadores Estefam e Jesus:

> O comportamento proibido consiste em desobedecer à ordem do funcionário público, i.e., desatender, não cumprir. Pode ser realizado mediante ação ou omissão, segundo consista o conteúdo da ordem em conduta positiva ou negativa do desobediente. Se a ordem impõe uma ação, a desobediência pode consistir em omissão, e vice-versa. O funcionário deve emitir uma ordem. Inexiste delito quando se trata de simples pedido e não de ordem. A ordem deve emanar de funcionário competente. Se incompetente, inexiste delito. Deve ela ser transmitida diretamente ao destinatário (verbalmente ou por escrito)

Portanto, esclarece as diversas formas da conduta de desobedecer à autoridade, não comumente espera uma ação ativa como os demais crimes tipificados no código penal, mas há também a conduta omissa para que se consuma também.

3.2.2 O crime de desobediência por parte dos provedores de internet

Superada a análise acerca do crime de desobediência de forma geral, cumpre destacar que esse delito pode assumir contornos mais gravosos quando se refere ao descumprimento de ordens emanadas de autoridade judicial ou policial. Nesses casos, o ordenamento jurídico prevê consequências mais severas, dada a relevância e a imperatividade dessas ordens no âmbito do Estado Democrático de Direito.

A maior gravidade atribuída a tais condutas decorre da necessidade de preservação da autoridade das instituições responsáveis pela manutenção da ordem pública e da efetividade das decisões judiciais, as quais possuem caráter cogente e vinculativo. Assim, tanto pessoas

físicas quanto jurídicas estão sujeitas ao cumprimento dessas determinações, sob pena de responsabilização penal e, eventualmente, civil ou administrativa, conforme o caso concreto.

Com isso, a possibilidade de autoridades requisitarem dados cadastrais diretamente dos provedores de internet, sem a necessidade de autorização judicial, suscita debates relevantes quanto à sua natureza jurídica. Em especial, questiona-se se tal requisição se encaixa no conceito de "ordem legal" prevista no artigo 330 do Código Penal, que tipifica o crime de desobediência.

Nos termos do artigo 10, §3º do Marco Civil da Internet (Lei nº 12.965/2014), delegados de polícia e membros do Ministério Público podem solicitar diretamente informações cadastrais, como nome, filiação e endereço de usuários de serviços de internet, sem prévia autorização do Poder Judiciário. Essa previsão normativa é interpretada por uma parcela da doutrina como uma delegação válida de competência legal às autoridades mencionadas, o que, a princípio, atribuiria legitimidade à requisição e a qualificaria como uma ordem legal.

Contudo, essa interpretação não é unânime, há entendimentos que apontam para a necessidade de se considerar não apenas a origem da ordem, mas também a legalidade formal e material do conteúdo requisitado. Isso porque, embora a lei autorize a requisição de dados básicos, ela não define claramente os limites entre o que é dado meramente cadastral e o que pode envolver dados de conexão ou de conteúdo, cuja requisição exige autorização judicial, conforme o próprio Marco Civil determina.

Ademais, do ponto de vista constitucional, o princípio da legalidade, a proteção da intimidade e a autodeterminação informativa exigem interpretação restritiva quando se trata de acesso estatal a dados pessoais. Assim, mesmo diante da autorização expressa na lei, há quem sustente que, na ausência de uma motivação adequada e proporcional da requisição, ela não se reveste dos requisitos mínimos para ser considerada legítima, o que afastaria a tipificação penal por desobediência, caso o provedor se recuse a fornecer as informações.

3.3 O conflito entre direito à privacidade e o interesse público na investigação criminal

Como visto no referido contexto, há uma espécie de conflito entre normas, evidenciando a complexidade da convivência entre diferentes dispositivos legais em um mesmo ordenamento jurídico. A busca pelo equilíbrio jurídico, se é que ele existe plenamente, muitas vezes passa pela necessidade de ponderação, em que um direito poderá ceder espaço ao outro, conforme as peculiaridades do caso concreto. Nesse escopo, é comum a ocorrência

de direitos em colisão, especialmente em situações nas quais dois princípios constitucionais ou legais entram em rota de confronto, como, por exemplo, a liberdade de expressão em comparação ao direito à intimidade. Nesses casos, não se trata de anular um direito em favor do outro, mas sim de harmonizá-los, de modo que ambos possam coexistir na maior medida possível.

3.3.1 Antinomia Jurídica

Por conseguinte, quando esse tipo de circunstância acontece, ocorre a denominada antinomia jurídica, que consiste no conflito de duas ou mais normas jurídicas, ou seja, essas normas determinam soluções diferentes ou contraditórias para um mesmo caso concreto, impossibilitando a aplicabilidade de ambas simultaneamente sem que gere incoerência no ordenamento jurídico.

Por conseguinte, quando esse tipo de circunstância acontece, ocorre a denominada antinomia jurídica, que consiste no conflito entre duas ou mais normas jurídicas válidas, as quais determinam soluções distintas ou até contraditórias para um mesmo caso concreto. Tal contradição torna inviável a aplicação simultânea dessas normas, sob pena de comprometer a coerência, a segurança e a harmonia do ordenamento jurídico.

Com isso, a antinomia pode ser classificada como real ou aparente, respectivamente, o conflito é profundo e não se resolve por simples interpretação, exigindo intervenção legislativa ou judicial para que se determine qual norma deve prevalecer, já nas aparentes, o conflito é somente superficial e pode ser solucionado por meio de critérios tradicionais de interpretação, como os princípios da especialidade, hierarquia e cronologia.

No tocante aos critérios de solução de antinomias normativas, o primeiro a ser considerado é o critério hierárquico, segundo o qual a norma inferior não pode contrariar a norma superior, sob pena de ser considerada inválida. Nesse sentido, a Constituição Federal de 1988, enquanto norma suprema do ordenamento jurídico brasileiro e vértice da pirâmide normativa proposta por Hans Kelsen, impõe-se como parâmetro de validade das demais normas infraconstitucionais. Assim, toda norma infralegal ou infraconstitucional deve estar consoante os preceitos constitucionais, sob pena de ser declarada inconstitucional, com consequente perda de eficácia e aplicabilidade.

Já o segundo critério diz respeito ao tempo, cronologia, entende-se que quando se há leis tratando da mesma matéria integralmente, a lei posterior revoga a anterior por questões de melhor adequação em relação ao tempo, a realidade social contemporânea. Ato contínuo, o

terceiro é a especialidade, dispõe que a norma especial prevalecerá sobre a norma geral, ainda que esta última seja posterior no tempo, pois, a especial disporá de uma situação específica de forma mais adequada. De modo que, não necessariamente a norma geral será revogada, elas podem coexistir.

Conforme o exposto, esse fenômeno evidencia a dinamicidade e complexidade do Direito, especialmente em sistemas jurídicos extensos, como o brasileiro, em que a produção legislativa é intensa e multifacetada. Assim, cabe ao intérprete do Direito, com base no caso concreto, nos princípios constitucionais e nas técnicas de hermenêutica ponderar os valores em jogo, buscando aplicar a norma que melhor atenda à justiça, à razoabilidade e ao interesse público, preservando a unidade e a funcionalidade do sistema jurídico na totalidade, se embasando pelos princípios da razoabilidade e da proporcionabilidade, adequando-os ao caso concreto.

3.3.2 Do conflito entre a privacidade e a investigação criminal

No contexto da temática, a antinomia ocorre na modalidade aparente, ao haver o direito a privacidade de um lado, e, em contrapartida, a segurança pública do outro, um direito individual conflitando com um direito coletivo, duas normas expressas na Constituição Federal de 1988, respectivamente nos artigos, 5º da CF/88, X e XII e o art. 144 , dispondo:

> Art. 144 - A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio.

Conforme exposto, a segurança pública é um dos pilares para manutenção do Estado Democrático de Direito, trata-se de um direito fundamental do cidadão, sendo dever do Estado a garantia da segurança pública, porém conforme supracitado, é responsabilidade de todos, sendo estes: poder público e sociedade civil, para que assim haja a garantia da ordem pública, a incolumidade das pessoas e a proteção do patrimônio.

Esse constante embate entre a segurança pública e o direito à privacidade do indivíduo evidência a complexidade das relações entre normas constitucionais e princípios fundamentais, revelando a tensão existente entre o interesse coletivo e os direitos individuais. De um lado, o Estado, por meio de suas instituições de segurança, exerce seu poder-dever de promover diligências investigativas visando garantir a ordem pública e prevenir ilícitos penais. De outro lado, há a necessidade de resguardar a esfera privada do cidadão, assegurando-se que o exercício da atividade estatal não resulte em arbitrariedades ou exposições indevidas.

Nessa perspectiva, eventual requisição de dados por autoridades públicas a provedores de internet, com o propósito de identificar possíveis suspeitos, pode representar violação à intimidade e dignidade da pessoa humana, sobretudo se a informação fornecida não corresponder de fato à identidade do verdadeiro investigado. Tal situação pode implicar constrangimento ou vexame indevido, acarretando prejuízos morais ao indivíduo exposto indevidamente à investigação. Assim, a atuação estatal deve observar critérios de legalidade, necessidade, proporcionalidade e fundamentação adequada, de modo a compatibilizar o interesse público com a preservação dos direitos fundamentais.

4 A JURISPRUDÊNCIA BRASILEIRA E O FORNECIMENTO DE DADOS CADASTRAIS

A jurisprudência brasileira permite nortear demais julgados, desempenhando um papel fundamental no contexto jurídico, ao ser através dela que se põe limites ou não em determinadas pautas acerca do que prevalecerá, assim como aborda o presente tema, consistindo sobre condições de compartilhamento de dados cadastrais, mediante casos concretos que vem acontecendo constantemente, os tribunais decidem de uma forma, ao passo que se é debatido todos os detalhes da temática. Desse modo, a presente seção analisa as principais decisões dos tribunais sobre a temática, abordando os direitos fundamentais envolvidos, bem como a interpretação das normas e os critérios adotados para chegar ao entendimento dos tribunais.

4.1 Decisões do Supremo Tribunal Federal (STF) sobre privacidade e investigação criminal

Sabe-se que a jurisprudência tem um papel fundamental no cenário jurídico, seja para dirimir conflitos de normas, para posicionamentos acerca de diversos assuntos e afins. Com o avanço tecnológico e a crescente virtualização das relações sociais e comerciais tornaram a proteção e o fornecimento de dados cadastrais muito vulneráveis, tendo em vista a facilidade em acessá-los e o mundo digital o qual as pessoas são imersas atualmente, com isso, sendo temas de grande relevância no cenário jurídico brasileiro por haver conflito entre normas, sendo estas: a privacidade dos cidadãos, o fornecimento de informações para investigações, e a segurança pública.

4.1.1 Teoria Tridimensional do Direito e a Jurisprudência

Com isso, partindo da Teoria Tridimensional do Direito desenvolvida por Miguel Reale, onde, entende que o direito possui três elementos independentes que consistem em fato, valor e norma, de modo que o Direito não se limita a um único aspecto isolado, o que se correlaciona também com a conceituação de dados, que igualmente não se restringem a uma única dimensão, buscando uma visão mais abrangente acerca dos fenômenos jurídicos.

Assim, destaca Miguel Reale (2003):

> Direito não é só norma, como quer Kelsen, Direito, não é só fato como rezam os marxistas ou os economistas do Direito, porque Direito não é economia. Direito não

> é produção econômica, mas envolve a produção econômica e nela interfere; o Direito não é principalmente valor, como pensam os adeptos do Direito Natural tomista, por exemplo, porque o Direito ao mesmo tempo é norma, é fato e é valor (2003, p.91)

Desse modo, destrinchando o conceito por Miguel Reale, o fato, é tudo que acontece no mundo real, ou seja, acontecimentos sociais, políticos, econômicos e culturais que fazem parte da vida em coletividade, contudo, nem todo fato se torna relevante para a área jurídica, para que isso ocorra é necessário que a sociedade atribua algum valor, isto significa que, tal fato seja importante para a coletividade, conforme o caso concreto, podendo requerer da sociedade a atenção, reprovação e afins, a depender do contexto.

Por conseguinte, a partir do momento em que um fato recebe valor, há a necessidade da criação da norma jurídica, visando a regulamentação daquele fato valorado, com intuito de preservar e garantir os direitos e deveres impostos a todos, bem como assegurar a justiça, em resumo, pode-se dizer que a Teoria Tridimensional de Reale, está dentro da expressão normatividade da realidade social valorada.

Contextualizando com a jurisprudência, ocorre esse mesmo processo, pois decisões reiteradas dos tribunais não nascem do acaso, mas sim de situações fáticas que ocorrem com frequência, quando certos litígios se tornam recorrentes, é percebido um padrão de comportamento social ao serem julgados, recebendo assim uma valoração jurídica pelo Poder Judiciário, subsequentemente essas decisões compõem entendimentos consolidados que posteriormente passam a influenciar novas decisões em casos semelhantes, contribuindo para harmonização das interpretações à aplicação das normas.

A exemplo dos conceitos supramencionados à temática, a crescente utilização da internet e das redes sociais que destrinchando ficaria como o uso da internet sendo fato, pois se tratava de um fenômeno novo e sem previsão legal, e com o decorrer do tempo surgiram várias situações que afligiram a sociedade sendo caracterizadas como crimes virtuais, fraudes, discursos de ódio, violações de privacidade e afins.

Conexo a isso, essa importância da coletividade atribuindo valor negativo a tais condutas, fora necessário que a partir dessa valoração em busca de dirimir os casos que vinham acontecendo, que, possivelmente, lesavam algum patrimônio, o legislador criou normas específicas para regulamentar acerca das situações, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Logo, os indivíduos faziam no ambiente virtual atitudes que no mundo real são condutas criminosas, mas como não existia legislação para esse cenário, nada do que era feito era punido como deveria, não ocorria a harmonização entre o mundo real e o mundo virtual, de forma que por muitas vezes, a internet era regida pelo ditado

“Terra sem lei”.

O Direito não precede os fatos sociais, mas tem sua função de resposta a eles, pois somente com fatos será criada uma norma, não tem a possibilidade do Direito prevê algo que nunca foi visto, a previsão legislativa ocorre justamente porque já houve acontecimentos naquele sentido, de modo que posteriormente passa a prevê os possíveis fatos naquele contexto, por isso se chama previsão legal, pois nesse caso já há uma norma e realmente está prevendo que tal conduta é criminosa, nesse sentido o Direito busca prevenir a reincidência de comportamentos prejudiciais, que atualmente são normatizados na ideia de prevenção, assim, o direito vive a reboque da sociedade, com novas ações ou omissões, consequentemente, novas leis, corroborando com a Teoria Tridimensional do Direito.

No exemplo prático relacionado à internet, correlacionado com a Teoria Tridimensional do Direito e jurisprudências, é o contexto atual, as decisões que os tribunais vem tomando, se algo está de fato consolidado. Contudo, antes de atingir esse estágio, houve um longo período de discussões sobre a temática. Nesse sentido, a evolução histórica das decisões pode ser compreendida a partir da ordem cronológica de algumas discussões iniciais que serão expostas a seguir no contexto de investigações criminais.

4.1.2 Decisões no âmbito do fornecimento de dados cadastrais

Em 16 de outubro de 2024 foi retomada a discussão sobre a possível autorização do Poder Judiciário em determinar a quebra de sigilo de dados de navegação de usuários na internet de maneira genérica, sem a devida cautela de individualização de cada usuário possivelmente envolvido. O tema foi debatido no Recurso Extraordinário (RE) 1301250, apresentado pela empresa Google (Google Brasil Internet Ltda. e Google LLC), de forma que a solução fora aplicada aos demais casos semelhantes.

O referido debate se deu por conta de uma decisão proferida pelo judiciário do Rio de Janeiro, que nas investigações do assassinato de Marielle Franco e seu motorista, Anderson Gomes, fora determinado pelo judiciário a quebra de sigilo de todas as pessoas que realizaram pesquisas na internet sobre Marielle Franco e sua agenda nos dias anteriores ao crime, e por isso envolve a colaboração da empresa Google, haja vista que, é uma empresa de tecnologia mundialmente famosa, mas principalmente conhecida pelos seus mecanismos de buscas, porém não se limita a somente isso, seus serviços vão além de uma busca no navegador.

Contudo, a Google é uma empresa que tem que se nortear também pela LGPD, a Constituição Federal de 1988 e pelo Marco Civil da Internet, tendo em vista que, seu trabalho

é exercido no mundo virtual, dessa forma, como fora decretado a quebra de sigilo de forma genérica, qualquer pessoa que tivesse feito algum tipo de busca como “Marielle Franco”, “vereadora Marielle”, “agenda da vereadora Marielle” e até mesmo o endereço “Rua dos Inválidos”, ou seja, qualquer indivíduo poderia ter pesquisado essas palavras-chave e ser alvo de investigação pela simples busca que poderia ser somente uma dúvida ou questionamento sobre Marielle.

Ocorre que, essa decisão levantou questionamentos legais e constitucionais pela empresa Google, considerando que, como supramencionado, a empresa tem que seguir a LGPD, a Constituição Federal, bem como o Marco Civil da Internet, desse modo, suprimiriam uma proteção que é de responsabilidade deles, considerando que, esse tipo de empresa tem o dever de guardar informações sigilosas, e ferindo consequentemente o direito à privacidade que não fora observado sua proteção constitucional, pois a decisão lesou vários direitos previstos por essas legislações, dentre essas, o art. 5º da Constituição Federal de 1988, incisos X e XII.

Com isso, essa decretação feriu o referido artigo, em seus incisos, presente na gama de Direitos e Garantias Fundamentais, nota-se que não houve individualização, de forma que essa violação foi em grande escala, pois qualquer pessoa poderia tirar uma dúvida no Google e pesquisar “Marielle Franco”, com isso, fere tanto a privacidade de cada indivíduo, quanto ao devido processo legal, podendo pensar em até o questionamento da presunção de inocência, pois algumas diligências só podem ser de fato realizadas quando se há algum ou alguns tipos de indícios referente ao caso que se busca solucionar.

O princípio da proporcionalidade é algo a ser questionado também nesses casos, haja vista, que envolve vários indivíduos que sequer comprovadamente têm algum tipo de participação no crime, por se tratar de investigação criminal fora decretado dessa forma, além de ter sido um crime de repercussão mundial, se faz necessário o uso da proporção entre o direito de cada indivíduo, sua privacidade, a sua intimidade, e a segurança pública. Ademais, foi um crime contra uma mulher, (que vitimou também seu motorista que estava no momento do crime), que exercia com empenho atividades políticas, fazendo com que toda a população brasileira se comoveu com o caso, pois era internacionalmente conhecida.

Por tratar-se de um decreto genérico, não individualizado, acaba que a investigação priorizou a segurança pública optando por trazer de imediato uma tranquilidade a sociedade, bem como solucionar um caso de grande repercussão que envolve durante o percurso várias fontes de mídia transmitindo informações, desse modo, o que ocorreu lesa também o que está previsto no Marco Civil da Internet, Lei 12.965/2014, conforme disposição a seguir:

> Art. 7º, III – Garante a inviolabilidade e sigilo do fluxo de comunicações e dos registros, salvo mediante ordem judicial específica.

Além disso, há uma série de requisitos para ocorrer essa determinação, assegurando assim, a proteção de cada usuário que possivelmente não estão em posições de criminosos, apesar de ter cumprido com os requisitos, fora tudo muito superficial quanto a aplicação dessa diligência que, segundo o Marco Civil da Internet, deve pautar-se nos seguintes critérios:

> Art. 10 – Determina que o fornecimento de registros deve ser precedido de ordem judicial fundamentada e com escopo definido.
> Art. 10, §1º – A autoridade judicial deve especificar "o motivo da requisição, o período de tempo a que se referem os registros, a identificação do responsável pela requisição e o tipo de registros requeridos".

Partindo dessa exposição, com relação ao debate, a referida medida para questões investigativas fora mantida pelo Tribunal do Rio de Janeiro (TJ-RJ) e pelo Superior Tribunal de Justiça (STJ), entendeu que a ordem estava devidamente fundamentada, haja vista, o acontecimento do crime, e reconhecendo igualmente que não se tratava de desproporcionalidade, pois, havia sido delimitado parâmetros de pesquisa, com determinação da região em período específico. Bem como, fora explanado acerca da restrição dos Direitos e Garantias Fundamentais para investigações criminais de crimes contra a vida, ademais, em crimes de impacto global, também foi ressaltado não haver risco para pessoas eventualmente afetadas, no quesito de se adequarem com as palavras supracitadas, tempo e local de pesquisa, uma vez que se não for constatada algum tipo de ligação com o fato ocorrido, as informações serão descartadas.

Contudo, pessoas que estão nessa alçada de não ter nenhuma conexão com o crime, trazem consigo um sentimento de violação de seus direitos, justamente, por serem indivíduos que possivelmente não fariam esse tipo de coisa e estão sendo investigadas em um crime internacionalmente conhecido, atingindo assim, o princípio da presunção da inocência.

Vale ressaltar que a empresa Google, esclareceu que essa medida atingia pessoas em grande escala, incluindo pessoas inocentes, e que o período de buscas foi firmado em 96 (noventa e seis horas), o que seria um período de 4 (quatro) dias, igualmente, fora considerado que a decisão tinha cunho genérico, fazendo com que demais decisões sobre qualquer temática fossem abarcadas por ela.

Portanto, é notório que o entendimento do STJ embora embasado de ponderações acerca da razoabilidade e da proporcionalidade, buscando harmonizar os Direitos em conflito, o direito coletivo ganha força em face do direito individual, em vista do bem da segurança pública, a qual alcança toda a sociedade, sendo dever do Estado exercê-la.

4.2 A Evolução Jurisprudencial no equilíbrio entre direitos fundamentais e segurança pública

A priori, uma das primeiras notícias com relação a dados, com base em pesquisa realizada no site do STF, fora em 08 de janeiro de 2008, versava sobre a desobrigação da empresa de telecomunicações Claro em fornecer dados cadastrais de clientes sob investigação, de modo que de início, se tem algo pendendo pro lado do direito da privacidade dos usuários. Segundo o ministro Gilmar Mendes, apesar do Supremo Tribunal Federal (STF) entender que o sigilo de dados não se trata de um direito absoluto, podendo ceder aos demais direitos, a quebra das informações deve ocorrer com o devido procedimento, seguindo a lei e o princípio da razoabilidade, a fim de evitar eventuais abusos.

A decisão fora liminar, concedida e uma ação cautelar (AC 1928) ajuizada pela Claro, Gilmar Mendes chegou a citar o julgamento recente da corte como embasamento, que consistia na vedação de acesso irrestrito pelo Tribunal de Contas da União (TCU), aos dados como Sisbacen, o Sistema de informações do Banco Central (BACEN).

Desse modo, a decisão fora tomada por meio de uma análise de um Mandado de Segurança (MS 22801) impetrado pelo BACEN, com isso, o STF ratificou a necessidade do acesso de dados constitucionalmente protegidos ocorra mediante uma motivação em casos específicos.

No mesmo sentido em 7 de maio de 2020, no site de notícias do STF, fora decidido acerca da suspensão dos efeitos da Medida Provisória (MP) 954/2020 que consistia em autorizar o compartilhamento de dados dos usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para que assim fosse realizada a produção de estatística na época do da COVID-19. Em plenário fora entendido que o compartilhamento supracitado, violava os direitos fundamentais, previsto na constituição em seu artigo 5º, incisos X e XII, os quais já foram supracitados, o que é perceptível a observância em priorizar o direito a privacidade, sigilo de informações, bem como, dados pessoais.

Por conseguinte, fora discutido a questão da divergência de direitos, pois segundo a Ministra Rosa Weber embora naquela época estivessem enfrentando uma crise sanitária gravíssima, não adiantaria, no combate a pandemia o atropelo de Direitos e Garantias Fundamentais positivados na Constituição Federal.

Posteriormente fora pontuado também que analisando a decisão tomada por maioria de votos entendendo pela suspensão, entraram no quesito de razoabilidade e proporcionalidade, pois os Direitos e Garantias Fundamentais presentes na Constituição Federal não são absolutos, isto é, podendo sofrer limitações quando se encontram em conflito com outros

direitos, que possivelmente estarão também protegidos pela Constituição. Entrando na questão supramencion ada, o ministro Alexandre de Moraes entendeu que não se tratava de algo razoável.

Na mesma corrente, o ministro Gilmar Mendes ressalta que o regulamento sanitário internacional da Organização Mundial da Saúde (OMS), presente no ordenamento jurídico brasileiro por meio do Decreto n. 10.212/2020, veda o tratamento de dados desnecessários e incompatíveis com a finalidade específica.

4.2.1 A delimitação promovida pela ADI 4906

Posteriormente, conforme pesquisado, fora conferido no site do STF, algumas repercussões do ano passado (2024), de causas a efeitos, houve um julgamento da Ação Direta de Inconstitucionalidade (ADI) 4906, fora entendido pelo STF que é constitucional o dispositivo de lei que permite que as autoridades policiais e Ministério Público podem, sim, requisitar de empresas de telefonia de dados cadastrais de pessoas investigadas sem a necessidade de uma ordem judicial.

A ADI supracitada busca equilibrar e limitar as coisas a fim de não deixar brecha para possíveis conflitos, pois embora houvesse discussões acerca da temática, nunca se falou em limitações do que poderia ser feito sem determinação judicial, e se algo de fato poderia ser feito.

Desse modo, a referida ação foi movida pela Associação Brasileira de Concessionárias de Serviço Telefônico Fixo Comutado (Abrafix), contra o art. 17 B da Lei de Lavagem de Dinheiro (Lei 9.613/1998), inserida pela Lei 12.683/2012, estabelece que autoridades e o Ministério Público podem ter acesso a dados cadastrais de investigados sem que haja uma prévia autorização judicial.

Portanto, é relevante salientar que, a partir da ação promovida pela ABRAFIX, para esclarecer o conceito de “dados cadastrais” passíveis de requisição direta por autoridades policiais e pelo Ministério Público, a decisão proferida pelo Supremo Tribunal Federal teve significativa repercussão. Isso porque o julgamento estabeleceu parâmetros objetivos quanto ao tipo de informação que pode ser compartilhada sem necessidade de autorização judicial, promovendo maior segurança jurídica e prevenindo eventuais abusos decorrentes de interpretações ampliadas ou equivocadas por parte dos provedores, ou das autoridades requisitantes.

5 CONCLUSÃO

Por todo o exposto, buscou-se analisar de forma crítica, à luz das legislações acerca da recusa dos provedores de internet em fornecer dados cadastrais mediante requisição da autoridade policial, e se é imprescindível haver ordem judicial para tal ato administrativo, por conseguinte, se essa negativa dos provedores possibilita o enquadramento dessa conduta como crime de desobediência, trazendo elementos detalhados dessa tipificação.

Partindo do entendimento de que a proteção de dados pessoais, especialmente diante do avanço tecnológico e da crescente digitalização das relações, é um direito fundamental vinculado à dignidade da pessoa humana, examinou-se o papel da Lei Geral de Proteção de Dados e do Marco Civil da Internet na regulação do uso, guarda e tratamento dessas informações. Paralelamente, abordou-se o interesse público na persecução penal e a necessidade de rápida obtenção de dados em investigações criminais.

Desse modo, embora a requisição direta de dados cadastrais por parte das autoridades policiais esteja previsto no ordenamento jurídico, fora possível notar que há lacunas quanto a sua delimitação de dados a fornecer, o dispositivo não traz clareza em detalhes quanto sua conceituação em relação à previsão do art. 10 parágrafo 3, bem como há muita divergência entre os doutrinadores quanto essa requisição ser sem prévia ordem judicial.

Nesse contexto, a recusa injustificada por parte dos provedores em atender a requisições legalmente fundamentadas, configura o crime de desobediência, desde que respeitados os critérios de legalidade, competência da autoridade e pertinência da ordem, pois até mesmo quanto a registros de informações, provedores podem ser punidos caso não haja essa guarda, que serve justamente para possíveis e posteriores requisições.

Assim, a monografia propôs como solução a necessidade de harmonização normativa, com melhor delimitação legal dos tipos de dados que podem ser acessados sem ordem judicial, a definição clara das autoridades competentes para a requisição, o fortalecimento dos mecanismos de controle, transparência e responsabilização de todos os agentes envolvidos, a análise de cada caso concreto e o uso dos princípios da proporcionalidade e razoabilidade, bem como a advertência para com os provedores sob o enquadramento da recusa no crime tipificado no art. 330 do código penal, haja vista a obstrução da celeridade e eficiência por parte da Administração Pública, de forma que obsta todo o processo investigativo.

Conclui-se, portanto, que a chave para o equilíbrio entre a proteção da privacidade e a efetividade da investigação criminal está na atuação responsável, legalmente fundamentada e tecnicamente precisa tanto dos órgãos de segurança pública quanto dos provedores de

internet, pois esses agem em função complementar para o uso de informações nas investigações criminais em consonância com os princípios constitucionais e os direitos fundamentais do cidadão, para evitar qualquer tipo de abuso e situações vexatórias para todo e qualquer envolvido nessa circunstância.

REFERÊNCIAS

BIONI, B. R. **Proteção de dados pessoais.** 2. ed. Rio de Janeiro: Forense, 2019.

BITENCOURT, C. R. **Tratado de direito penal**: parte especial. v. 5. 18. ed. Rio de Janeiro: Saraiva Jur, 2024. E-book. p. 182. ISBN 9786553629264. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553629264/. Acesso em: 11 jun. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União: seção 1,** Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 11 jun. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Di**ário Oficial da União: seção 1,** Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 11 jun. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União:** seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jun. 2025.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: **seção 1,** Brasília, DF, 12 maio 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 11 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União: seção 1**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jun. 2025.

BRASIL. MINISTÉRIO DA SAÚDE. **Classificação dos dados pessoais.** Disponível em: https://www.gov.br/saudedobrasil/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acesso em: 11 jun. 2025.

CAPEZ, F**. Curso de direito penal: parte especial, arts. 213 a 359-T.** v. 3. 21. ed. São Paulo: Saraiva, 2023.

GONÇALVES, V. H. P. **Marco Civil da Internet comentado.** 1. ed. Rio de Janeiro: Atlas, 2017. E-book. p. 100. ISBN 9788597009514. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788597009514/. Acesso em: 11 jun. 2025.

GUERREIRO, R.; TEIXEIRA, T. **Lei Geral de Proteção de Dados Pessoais**. 4. ed. São Paulo: Saraiva, 2022.

JESUS, D. E. de; OLIVEIRA, J. A. M. de. **Marco Civil da Internet: comentários à Lei nº 12.965, de 23 de abril de 2014**. 1. ed. Rio de Janeiro: Saraiva, 2014. E-book. p. 50. ISBN 9788502203200. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502203200/. Acesso em: 11 jun. 2025.

JOTA. **STF define critérios para telefônicas compartilharem dados com a polícia.** Disponível em: https://www.jota.info/stf/do-supremo/stf-define-criterios-para-telefonocas-compartilharem-dados-com-a-policia. Acesso em: 23 nov. 2024.

LEITE, G. S.; LEMOS, R. **Marco Civil da Internet.** 1. ed. Rio de Janeiro: Atlas, 2014. E-book. p. 158. ISBN 9788522493401. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788522493401/. Acesso em: 11 jun. 2025.

MASSON, C. **Direito penal: parte especial – arts. 213 a 359-T**. v. 3. 15. ed. Rio de Janeiro: Método, 2025. E-book. p. 657. ISBN 9788530995898. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530995898/. Acesso em: 11 jun. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **STF valida dispositivo da Lei de Lavagem de Dinheiro que permite acesso a dados cadastrais de investigados sem autorização judicial**. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr2/2024/stf-valida-dispositivo-da-lei-de-lavagem-de-dinheiro-que-permite-acesso-a-dados-cadastrais-de-investigados-sem-autorizacao-judicial. Acesso em: 10 nov. 2024.

MONTEIRO, R. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?.** Rio de Janeiro: Instituto Igarapé, 2018. (Artigo Estratégico 39).

REALE, M. **Teoria tridimensional do direito**. 5. ed. São Paulo: Saraiva, 2003.

SOLER, F. G. **Proteção de dados: reflexões práticas e rápidas sobre a LGPD**. São Paulo: Saraiva, 2021.

SUPREMO TRIBUNAL FEDERAL (STF). **Associação pede que STF valide necessidade de ordem judicial para acessar registros de usuários na internet.** Disponível em: https://noticias.stf.jus.br/postsnoticias/associacao-pede-que-stf-valide-necessidade-de-ordem-judicial-para-acessar-registros-de-usuarios-na-internet/. Acesso em: 25 set. 2024.

SUPREMO TRIBUNAL FEDERAL (STF). **STF anula provas obtidas a partir de dados preservados em contas da internet sem autorização judicial**. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-anula-provas-obtidas-a-partir-de-dados-preservados-em-contas-da-internet-sem-autorizacao-judicial/. Acesso em: 10 nov. 2024.

SUPREMO TRIBUNAL FEDERAL (STF). **STF e proteção de dados pessoais: decisões da Corte marcaram a evolução de um novo direito fundamental**. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-e-protecao-de-dados-pessoais-decisoes-da-corte-marcaram-a-evolucao-de-um-novo-direito-fundamental/. Acesso em: 16 nov. 2024.

SUPREMO TRIBUNAL FEDERAL (STF). **Norma que autoriza MP e polícia a requisitar de telefônicas dados cadastrais de investigados é válida, decide STF.** Disponível em: https://noticias.stf.jus.br/postsnoticias/norma-que-autoriza-mp-e-policia-a-requisitar-de-telefonicas-dados-cadastrais-de-investigados-e-valida-decide-stf/. Acesso em: 11 jun. 2025.

SUPREMO TRIBUNAL FEDERAL (STF). **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE.** Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-suspende-compartilhamento-de-dados-de-usuarios-de-telefonicas-com-ibge/. Acesso em: 23 abr. 2025.

SUPREMO TRIBUNAL FEDERAL (STF***). Claro está desobrigada de fornecer dados cadastrais de clientes sob investigação***. Disponível em: https://noticias.stf.jus.br/postsnoticias/claro-esta-desobrigada-de-fornecer-dados-cadastrais-de-clientes-sob-investigacao/. Acesso em: 11 jun. 2025.

SUPREMO TRIBUNAL FEDERAL (STF). **Entenda: STF vai discutir quebra de sigilo de histórico de busca na internet em procedimentos penais [Caso Marielle].** Disponível em: https://noticias.stf.jus.br/postsnoticias/entenda-stf-vai-discutir-quebra-de-sigilo-de-historico-de-busca-na-internet-em-procedimentos-penais/. Acesso em: 24 abr. 2025.