PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

FACULDADE DE DIREITO

LETÍCIA DELFINO RODRIGUES

A NECESSIDADE DA CONDUTA ILÍCITA DO USUÁRIO PARA O FORNECIMENTO DE DADOS PELO PROVEDOR DE APLICAÇÕES DE INTERNET, À LUZ DA EMENDA CONSTITUCIONAL Nº 115/2022

TRABALHO DE CONCLUSÃO DE CURSO

SÃO PAULO – SP

2023

LETÍCIA DELFINO RODRIGUES

A NECESSIDADE DA CONDUTA ILÍCITA DO USUÁRIO PARA O FORNECIMENTO DE DADOS PELO PROVEDOR DE APLICAÇÕES DE INTERNET, À LUZ DA EMENDA CONSTITUCIONAL Nº 115/2022

Projeto de Trabalho de Conclusão de Curso apresentado à banca avaliadora da Faculdade de Direito da Pontifícia Universidade Católica de São Paulo, como parte dos requisitos necessários para obtenção do título de Graduado em Direito.

Orientadora: Profa. Nathaly Campitelli Roque

SÃO PAULO – SP

2023

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a Deus pela vida e pelo discernimento diário de seguir o caminho certo e do bem.

Em segundo lugar, agradecer a minha mãe, o meu pai, e o meu irmão. Aos meus pais, por sempre me induzirem a estudar e terem me dado a oportunidade de me formar na maior Faculdade de Direito do Brasil: a Pontifícia Universidade Católica de São Paulo. À minha mãe, por ter acompanhado de perto a minha graduação, me apoiado e vibrado por todas as minhas conquistas. Mãe, essa conquista é sua também. Obrigada! Pai, você sempre esteve certo: podem te roubar tudo, mas nunca o seu conhecimento. Ao meu irmão, pela parceria ao longo desses 23 anos e por sempre ter me guiado e reconhecido o meu esforço ao longo desses anos de estudo.

Agradeço também a Talita, minha prima, que despertou em mim o gosto pela leitura, pelos estudos e, principalmente, pela justiça. Tata, o encerramento dessa etapa tem grande influência sua. Obrigada!

Gostaria também de agradecer às amigas que estiveram comigo nessa jornada intensa e nunca me deixaram desistir. Ana Vitória, Amanda, Bárbara, Esther, Giovanna, Isabella, Juliana, Julia, Lia e Martina, vocês são as melhores amigas que eu poderia ter.

À minha orientadora Prof. Nathaly Campitelli Roque, por ter me auxiliado na elaboração desta pesquisa e, por fim, à Pontifícia Universidade Católica de São Paulo, por ter despertado em mim um dos meus maiores interesses: o Direito. Foi através das aulas ministradas por professores exemplares e da vivência pelo *campus* Monte Alegre que descobri que estava no caminho certo.

RESUMO

O presente trabalho de conclusão de curso visa analisar os impactos da Emenda Constitucional nº 115/2022, especificamente nos casos judiciais em que há pedido de fornecimento de dados direcionado ao provedor de aplicações de internet. O artigo 22 do Marco Civil da Internet estabelece requisitos que devem ser cumpridos no momento em que a parte requerente formula o pedido de fornecimento de dados de determinado usuário, sendo que um desses requisitos é a comprovação de ato ilícito cometido por esse usuário. Antes da Emenda Constitucional nº 115/2022, o pedido e o deferimento do fornecimento de tais dados sem a comprovação do ato ilícito violava meramente leis infraconstitucionais, que garantem ao usuário a privacidade e a proteção aos dados pessoais. A partir da Emenda Constitucional nº 115/2022, eventual deferimento sem a observação do ato ilícito gerou novos efeitos: a violação de um direito fundamental garantido constitucionalmente. Diante disso, verifica-se que os impactos de tal Emenda nos procedimentos judiciais onde se requer ao provedor de aplicações de internet dados de um usuário para identificá-lo são claros: o cuidado e a cautela ao se requerer os dados, bem como ao analisar o caso, deverão ser redobrados. Caso contrário, o usuário terá o seu direito fundamental de proteção aos seus dados pessoais violados.

Palavras-chave: Dados pessoais; provedor de aplicações de internet; direito fundamental; ato ilícito; emenda constitucional.

ABSTRACT

This conclusion work analyzes the impacts of Constitutional Amendment 115/2022, specifically in court cases in which there is a request for provision of data directed to the provider of internet applications. Article 22 of the Marco Civil da Internet establishes requirements that must be met when the requesting party formulates a request for data from a particular user, and one of these requirements is evidence of unlawful acts committed by the user. Before Constitutional Amendment No. 115/2022, the request and the granting of the provision of such data without evidence of unlawful acts only violated infra-constitutional laws that guarantee the user's privacy and the protection of personal data. After the Constitutional Amendment 115/2022, the eventual granting without the observation of the unlawful act generated new effects: the violation of a fundamental right constitutionally guaranteed. Therefore, it is clear that the impacts of the Amendment on judicial procedures where the provider of Internet applications is required to provide data from a user in order to identify him or her are clear: the care and attention when requesting the data, or when analyzing the case, should be doubled. Otherwise, the user will have his fundamental right to protection of his personal data violated.

Keywords: Personal data; Internet application provider; Fundamental right; Unlawful act; Constitutional amendment.

SUMÁRIO

INTRODUÇÃO…….6

1. PROVEDORES DE APLICAÇÕES DE INTERNET……...8

1.1 O SURGIMENTO DOS PROVEDORES DE APLICAÇÕES DE INTERNET E O SEU CONCEITO……...……..…….8

1.2 O MARCO CIVIL DA INTERNET E SEUS PRINCÍPIOS……..……...11

2. DADOS QUE OS PROVEDORES DE APLICAÇÕES DE INTERNET ESTÃO OBRIGADOS A ARMAZENAR E/OU FORNECER……..……...17

2.1 REGISTROS DE ACESSO……..……17

2.2 SUFICIÊNCIA DO REGISTROS DE ACESSO PARA IDENTIFICAÇÃO DE USUÁRIOS……...19

2.3 PRAZO LEGAL DE ARMAZENAMENTO DOS REGISTROS DE ACESSO……...21

3. O ARTIGO 22 DO MARCO CIVIL DA INTERNET: REQUISITOS LEGAIS PARA O FORNECIMENTO DE DADOS PELO PROVEDOR……24

3.1 ORDEM JUDICIAL, ATO ILÍCITO, JUSTIFICATIVA E PERÍODO……..24

3.2 A IMPORTÂNCIA DA COMPROVAÇÃO DO ATO ILÍCITO, SOB PENA DE VIOLAÇÃO AO ART. 22 E AO DIREITO DE PRIVACIDADE DO USUÁRIO……28

4. A EMENDA CONSTITUCIONAL Nº 115/22 E SEUS IMPACTOS NO FORNECIMENTO DE DADOS PELO PROVEDOR……31

5. CONCLUSÃO…….35

REFERÊNCIAS

INTRODUÇÃO

Com a globalização e o avanço da internet, as pessoas passaram a utilizar as redes sociais para os mais diversos objetivos, como conexão, *networking*, trabalho, o que causou uma adesão massiva às redes. Com isso, os provedores de aplicações de internet, que são os responsáveis por disponibilizar o ambiente da rede social aos usuários, passaram a coletar diversos dados de seus usuários, até porque o anonimato é vedado no ambiente virtual.

Assim, quando uma parte se vê lesada por outra através de um ato cometido no ambiente virtual, ela busca o Judiciário para identificar tal pessoa e, com isso, tomar as medidas cabíveis. Para que essa identificação seja feita, a parte deve requer ao provedor de aplicações de internet os dados que ele está obrigado a armazenar e fornecer, nos termos do artigo 15 do Marco Civil da Internet (Lei nº 12.965/2014).

No entanto, o Marco Civil da Internet, em seu artigo 22, parágrafo único, inciso I, determina a necessidade de uma conduta ilícita do usuário para o fornecimento de dados do mesmo pelos provedores de aplicações de internet. Dessa forma, quando há um pedido de fornecimento de dados no processo civil, seja em sede de liminar ou de mérito, é necessário que a parte autora comprove a ilicitude do ato praticado pelo proprietário do dado, a fim de viabilizar o fornecimento de seus dados pelo provedor de aplicações de internet.

Acontece que, com a promulgação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, a proteção de dados pessoais foi incluída entre os direitos e garantias fundamentais do indivíduo. Nesse sentido, o artigo 22 do Marco Civil da Internet ganha uma força ainda maior, na medida em que, caso o ilícito não esteja devidamente comprovado nos autos, não poderá haver o fornecimento dos dados pessoais, sob pena de se violar um direito fundamental do indivíduo.

Em outras palavras, desde a promulgação do Marco Civil da Internet, a ilicitude precisou ser comprovada para o fornecimento de dados de determinado usuário, por força do artigo 22, parágrafo único, inciso I, do Marco Civil da Internet, mas a promulgação da Emenda Constitucional nº 115/22 possui impacto nesses casos, uma vez que, se a ilicitude não estiver, de fato, comprovada, estar-se-á colocando em risco o direito e uma garantia fundamental do usuário.

Dessa forma, a presente pesquisa busca verificar os impactos da Emenda Constitucional nº 115/22 nas ordens judiciais que determinam aos provedores de aplicação de internet o fornecimento de dados de determinado usuário, especificamente quanto à necessidade da ilicitude na conduta do usuário para a quebra do sigilo de dados do mesmo.

A importância da presente pesquisa está no fato de que os dados pessoais estão cada vez mais em alta, bem como o armazenamento de tais dados pelos provedores de aplicações de internet. Assim, nada mais relevante do que analisar as mudanças legislativas e os seus impactos na prática.

De modo a verificar o questionamento supramencionado, delineou-se como objetivo geral verificar os ditames e os princípios que norteiam o Marco Civil da Internet, bem como analisar a importância da Emenda Constitucional nº 115/2022.

Como objetivos específicos, tem-se: conceituar os provedores de aplicações de internet; analisar os princípios do Marco Civil da Internet, especificamente os de privacidade e proteção dos dados pessoais; apontar quais os dados os provedores de aplicações de internet estão obrigados a armazenar ou fornecer; evidenciar os requisitos legais para o fornecimento de dados no processo judicial; evidenciar a importância da comprovação do ato ilícito, sob pena de violação ao artigo 22 e ao direito de privacidade do usuário; e, por fim, analisar a Emenda Constitucional nº 115/2022 e seus impactos no fornecimento de dados pelo provedor de aplicações.

A partir de pesquisas desenvolvidas sob o prisma do método de abordagem dedutivo, com base em bibliografias, estudos existentes sobre o tema, bem como na recente jurisprudência, o objetivo do presente trabalho é apontar os impactos da Emenda Constitucional nº 115/2022 no fornecimento de dados requerido em processo judicial ao provedor de aplicações de internet.

1. PROVEDORES DE APLICAÇÕES DE INTERNET

1.1 O SURGIMENTO DOS PROVEDORES DE APLICAÇÕES DE INTERNET E O SEU CONCEITO

A partir do século XXI, diversas mudanças sociais e tecnológicas deram origem à 4ª Revolução Industrial, também denominada Indústria 4.0. Através desse movimento, houve um avanço drástico da tecnologia, que deu origem a produtos como: impressoras 3D, algoritmo, inteligência artificial, biologia sintética, realidade aumentada, big data, entre outros.

Verifica-se que a característica principal de tal revolução está na fusão entre o mundo físico e o virtual, na medida em que as relações pessoais passaram a ter espaço em um âmbito cibernético. É evidente que todas essas alterações mudam radicalmente a sociedade e o modo de viver, assim como ocorreu em todas as outras revoluções industriais. Nas palavras de Marcelo Romão Marineli:

> "As duas últimas décadas, em particular, foram testemunhas de uma verdadeira revolução tecnológica ligada, justamente, ao desenvolvimento maciço dessas tecnologias de comunicação e informação, notadamente a internet, os computadores pessoais ligados à rede e os dispositivos móveis, como *tablets* e *smartphones*. Esse salto tecnológico imprimiu uma nova configuração de sociedade, permeando todos os aspectos da vida: social, econômico, político, cultural, entre outros"[1].

Com isso, a internet ganhou bastante relevância, inclusive as redes sociais. Isso porque, é através desses aplicativos - como Google, Youtube, Facebook, Instagram, LinkedIn, Twitter, Tiktok, WhatsApp, Pinterest, Tinder - que as pessoas trabalham, se relacionam, trocam dicas, compartilham conquistas e promovem conhecimento, com a facilitação de estarem em qualquer lugar do mundo.

Ou seja, você não precisa mais ir de porta em porta de empresas entregar currículo, por exemplo, se pode fazer isso através do LinkedIn, ou de um e-mail. Segundo Pierre Levý, "uma comunidade virtual é construída sobre as afinidades de interesses, de conhecimento, sobre projetos mútuos, em um processo de cooperação ou troca, tudo isso independentemente das proximidades geográficas e das filiações institucionais"[2].

---

[1] Privacidade e Redes Sociais Virtuais: Sob a égide da Lei nº 12.965/2014 - Marco Civil da Internet. 1. ed. Rio de Janeiro: Lumen Juris, 2017, p. 7.

[2] Cibercultura. Tradução Carlos Irineu da Costa. 7ª reimpressão. São Paulo, 34, 2008, p. 127.

Já para Thelma Fernandes de Novaes, "as redes sociais nasceram para integrar membros com interesses e ideologias ligados pela relevância de um determinado assunto e para proporcionar interatividade e integração por meio de compartilhamento de conteúdo"[3]. Por fim, Marcelo Marineli entende que:

> "As redes sociais virtuais, portanto, são serviços on-line, que têm como objetivo construir redes ou relações sociais entre pessoas, que compartilham interesses em comum. São espaços específicos na internet que abarcam verdadeiras estruturas sociais, compostas por pessoas que buscam o contato virtual fundado em afinidades e objetivos comuns"[4].

Com isso, é possível concluir que as redes sociais surgiram com o fito de facilitar a comunicação e a realização de determinadas atividades pelas pessoas, o que aproximou e facilitou a comunicação entre pessoas que possuem interesses em comum. Elas são plataformas que permitem aos indivíduos se conectarem, interagirem e partilharem informações uns com os outros, permitindo com que os usuários criem perfis pessoais, estabeleçam ligações com outros usuários e participem em várias formas de comunicação, tais como o envio de mensagens, o compartilhamento de conteúdos e a participação em comunidades.

Independentemente da forma que se conceitua as redes sociais, qualquer pessoa que vive no século XXI consegue mensurar a importância que elas possuem na rotina das pessoas. E, como se sabe, para que o acesso às redes seja viabilizado, é necessário criar um perfil, e é através desse perfil que o indivíduo informa dados pessoais necessários para a sua identificação na plataforma. A partir daí, passamos a entrar no conceito de provedores de aplicações de internet.

Os provedores de aplicações de internet são responsáveis por fornecer um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, conforme preceitua o artigo 5º, inciso VII, do Marco Civil da Internet (Lei nº 12.965/2014), ao conceituar as "aplicações de internet":

> Art. 5º Para os efeitos desta Lei, considera-se:
> (...)
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

---

[3] Identidade: as diversas faces de uma sociedade em rede. 2013. 97f. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) - Pontifícia Universidade Católica de São Paulo, São Paulo. 2013, p.63.
[4] Privacidade e Redes Sociais Virtuais: Sob a égide da Lei nº 12.965/2014 - Marco Civil da Internet. 1. ed. Rio de Janeiro: Lumen Juris, 2017, p. 19.

Dessa forma, verificamos que as redes sociais, em sua natureza jurídica, são nada mais, nada menos, que provedores de aplicações de internet, na medida em que fornecem um ambiente conectado à internet para que os usuários o acessem e desfrutem das especificidades que tal ambiente pode oferecer. Tarcisio Teixeira afirma que:

> "Apesar de o Marco Civil trazer em seu texto uma série de conceitos, sobretudo no seu art. 5º, ele optou por não conceituar o que vem a ser provedor. Provedor tem o sentido daquele que prove algo. Especificamente na rede mundial de computadores é a doutrina quem conceitua e classifica as várias espécies de provedores. O provedor de **serviços de internet** realiza uma atividade de prestação de serviços relacionados ao funcionamento da rede mundial de computadores, havendo muita confusão entre as espécies de provedores. Provedor de serviços de internet é um gênero do qual são espécies: provedor de *backbone*, provedor de acesso, provedor de correio eletrônico, provedor de hospedagem e provedor de conteúdo"[5].

Nas palavras de Marcelo Marinelli:

> "(...) E os provedores de aplicações são os que o autor denominou de provedores de informação ou conteúdo, responsáveis pelas páginas e funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet. Portanto, quanto à natureza jurídica das redes sociais virtuais, entendemos tratar-se de provedores de aplicações de internet, especificamente provedores de conteúdos, ou seja, são prestadores de serviços, pois criam um ambiente favorável para que os usuários disponibilizem informações, arquivos, opiniões e comentários"[6].

Já para Carlos Affonso Souza, Ronaldo Lemos e Celina Bottino:

> "Os provedores de aplicações de Internet podem ser compreendidos como a pessoa que fornece um conjunto de funcionalidades que são acessadas por meio de um terminal conectado à Internet. O provedor de aplicações de Internet aparenta englobar os tradicionalmente chamados provedores de conteúdo (que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da Internet, como, as redes sociais, os aplicativos de mensagens e as plataformas para compartilhamento de vídeo) e de hospedagem (que armazenam dados de terceiros, conferindo-lhes acesso remoto), tendo em vista que, no artigo 19 do MCI, foi determinado que a responsabilidade civil desse provedor, por conteúdo gerado por terceiro, será omissiva e a partir da notificação judicial"[7].

Vale ressaltar, ainda, que o próprio Superior Tribunal de Justiça já conceituou os provedores de aplicações de internet:

> "**Os provedores de serviços de Internet são aqueles que fornecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio**

[5] Marco Civil da Internet comentado. São Paulo: Almedina, 2016, p. 96.
[6] Privacidade e Redes Sociais Virtuais: Sob a égide da Lei nº 12.965/2014 - Marco Civil da Internet. 1. ed. Rio de Janeiro: Lumen Juris, 2017, p. 23.
[7] Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017, p. 96.

> **dela**. Trata-se de gênero do qual são espécies as demais categorias, como: (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade da Internet, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores backbone e revendem aos usuários finais, possibilitando a estes conexão com a Internet; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na Internet; e **(v) provedores de conteúdo, que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da web**"[8]. (grifos meus)

Diante dos conceitos apresentados, é possível aferir que os provedores de aplicações de internet são responsáveis por fornecer um conjunto de funcionalidades por meio de um terminal, como um computador conectado à internet. Assim, são prestadores de serviços que disponibilizam um ambiente conectado à internet para que os usuários o acessem e desfrutem das especificidades que tal ambiente pode oferecer. A título de exemplo, o provedor de aplicações dos serviços Facebook e Instagram é a Meta Plataforms, Inc., enquanto o provedor de aplicações do serviço Twitter é o Twitter, Inc.

Após classificar a natureza jurídica das redes sociais, verifica-se que a legislação aplicável aos provedores de aplicações de internet é o Marco Civil da Internet, que será abordado no subcapítulo seguinte.

1.2 O MARCO CIVIL DA INTERNET E SEUS PRINCÍPIOS

O Marco Civil da Internet tem como objetivo principal estabelecer "*garantias, direitos e deveres para o uso da internet no Brasil*" e determinar "*as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria*", nos termos do artigo 1º da lei. A legislação é demasiadamente importante por ser a primeira a tratar especificamente dos provedores de aplicações e conexões de internet, e passou a ser utilizada como fundamento para decisões em casos judiciais envolvendo tais provedores. O jurista Marcelo Marineli diz um pouco sobre a criação e a estruturação do Marco Civil da Internet:

> "No ano de 2011 o Poder Executivo apresentou perante a Câmara dos Deputados o Projeto de Lei nº 2.126/2011, que ficou conhecido como o Marco Civil da internet. Após três anos de tramitação, com consultas públicas realizadas e a instituição de uma Comissão Especial para a apreciação da matéria, em 23 de abril de 2014, o projeto foi aprovado e transformado na Lei nº 12.965/2014. O Marco Civil da internet é, atualmente, a lei que regula a utilização da internet no Brasil, criando uma moldura de direitos e deveres para os usuários e provedores da grande rede, bem

[8] REsp n. 1.316.921/RJ, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 26/6/2012, DJe de 29/6/2012

> como diretrizes para a atuação do Estado. (...) Mas é importante ficar claro que o Marco Civil da internet apenas traz as bases para a regulação. Coube ao Decreto nº 8.771, de 11 de maio de 2016, regulamentar a Lei nº 12.965/2014, tratando de tópicos como as hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, os procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, as medidas de transparência na requisição de dados cadastrais pela administração pública e os parâmetros para fiscalização de apuração de infrações"[9].

Para Damásio de Jesus, é:

> "Importante mencionar que no Brasil não existia lei específica que tratasse dos deveres dos provedores de acesso, aplicações e dos direitos dos usuários. Questões submetidas ao Judiciário comumente apresentavam decisões contraditórias e eram julgadas com base na aplicação do Código Civil Brasileiro, Código de Defesa do Consumidor e outras legislações existentes. Uma das funções do Marco Civil Brasileiro é gerar segurança jurídica, oferecendo base legal ao Poder Judiciário quando se deparar com questões envolvendo internet e tecnologia da informação, evitando-se decisões contraditórias sobre temas idênticos, o que era muito comum"[10].

Para Victor Hugo Pereira Gonçalves:

> "O Marco Civil é uma legislação cujo objetivo precípuo é o de regular as relações sociais entre os usuários de internet. A internet é um fenômeno tecnológico recente que alterou a forma das relações e a percepção social de situações que, no mundo físico, seriam simples e banais. Um simples comentário, depreciativo ou não, emitido na rua, propagava-se e perdia-se naquele momento. O mesmo comentário, na internet, fixa-se indefinidamente nos programas e servidores dela, que nunca se esquecerão e registrarão aquele simples evento para sempre"[11].

Assim, o Marco Civil da Internet surgiu com o objetivo de regular as relações e atividades virtuais que foram viabilizadas pela Indústria 4.0, as quais antigamente eram julgadas com base no Código Civil e no Código de Defesa do Consumidor, o que causava certa insegurança jurídica, na medida em que não havia lei específica que tratasse dos provedores de aplicações e suas relações com os usuários. Daí a importância do Marco Civil da Internet.

Esclarecida a relevância da referida lei, passar-se-á a realizar uma análise dos princípios que a norteiam, especificamente aqueles que dizem respeito à privacidade e à proteção dos dados pessoais. O artigo 3º da lei dispõe sobre tais princípios:

> Art. 3º **A disciplina do uso da internet no Brasil tem os seguintes princípios**:

---

[9] Privacidade e Redes Sociais Virtuais: Sob a égide da Lei nº 12.965/2014 - Marco Civil da Internet. 1. ed. Rio de Janeiro: Lumen Juris, 2017, p. 26.
[10] Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014, p. 18.
[11] Marco Civil da Internet comentado. 1. ed. São Paulo: Atlas, 2017. p. 6.

> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> **II - proteção da privacidade;**
> **III - proteção dos dados pessoais, na forma da lei**;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (grifos meus)

Verifica-se que o direito à privacidade e à proteção aos dados pessoais estão destacados tanto no inciso II quanto no inciso III do dispositivo acima, pois tais princípios passaram a ter ainda mais relevância no mundo virtual. Isso se deve a diversas razões, como (i) a grande quantidade de informações pessoais, na medida em que os provedores de aplicações de internet armazenam grande quantidades de dados pessoais dos seus milhares de utilizadores; (ii) compartilhamento de informações sensíveis nas redes sociais, como dados financeiros; e (iii) a ocorrência de violações de dados ou de acesso por pessoa não autorizada.

Diante desse contexto, as redes sociais passaram a ter uma maior atenção à privacidade e à proteção dos dados, realizando debates sobre a regulamentação da privacidade dos dados, o consentimento dos usuários, a transparência no tratamento dos dados, e a responsabilidade dos provedores de aplicações na salvaguarda das informações. Diante disso, surgiram as políticas de privacidade das redes sociais.

A título de exemplo, a Política de Privacidade do Twitter[12] dispõe que as informações coletadas são divididas em três categorias: (i) informações fornecidas pelo usuário, como nome de usuário, senha, endereço de e-mail, número de telefone, data de nascimento, localização, número de cartão de crédito e endereço de cobrança; (ii) informações coletadas pelo provedor quando o usuário utiliza a plataforma, como conteúdos postados, interações com outros usuários, mensagens privadas, data e hora de envio, endereço do IP, tipo de navegador utilizado, operadora utilizada pelo dispositivo, aplicativos instalados no dispositivo, nível de bateria, memória, e agenda de endereços; e (iii) informações recebidas de terceiros, como anunciantes, desenvolvedores e editores da plataforma.

Dado o exemplo, fica claro que os dados eventualmente armazenados são extremamente pessoais e caracterizam a individualidade de cada usuário. Assim, os

[12] Twitter Privacy Policy. Disponível em: https://twitter.com/en/privacy#twitter-privacy-1. Acesso em 08 de maio de 2023.

provedores coletam e armazenam milhares de dados de pessoas do mundo inteiro, e é claro que tais dados devem estar em um ambiente seguro, para que não sejam compartilhados com terceiros de forma ilícita. É nesse momento que o direito à privacidade e à proteção dos dados pessoais se destacam, na medida em que, ao compartilhar seus dados com o provedor, os mesmos devem ser tratados na forma da lei, de forma segura.

Além do artigo 3º mencionado anteriormente, o direito à privacidade e à proteção de dados pessoais ainda são mencionados em diversos momentos na lei, como nos artigos 7º, incisos I, II, III, VII, VIII, IX, X, 8º, *caput*, 10:

> Art. 7º **O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos**:
> I - **inviolabilidade da intimidade e da vida privada**, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - **inviolabilidade e sigilo do fluxo de suas comunicações pela internet**, salvo por ordem judicial, na forma da lei;
> III - **inviolabilidade e sigilo de suas comunicações privadas armazenadas**, salvo por ordem judicial; (...)
> VII - **não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet**, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - **informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais**, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - **consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais**, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - **exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes**, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (...) (grifos meus)

> Art. 8º **A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet**. (grifos meus)

> 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**. (grifos meus)

Além dos artigos mencionados acima, o princípio da privacidade também está constitucionalmente preconizado no artigo 5º, inciso X[13], da Constituição Federal, como

[13] 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

direito fundamental. E, como será melhor visto ao longo do trabalho, o direito à proteção de dados pessoais também se tornou um direito fundamental, através da Emenda Constitucional nº 115/2022.

Além disso, o Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, em seu artigo 13[14], dispõe sobre as diretrizes de padrões de segurança que devem ser observados pelos provedores de conexão e aplicações ao armazenar e tratar os dados pessoais coletados e as comunicações privadas. A título de exemplo, dispõe que o acesso aos dados deve ser restrito e exclusivo para determinadas pessoas.

Além disso, o parágrafo 2º do mesmo dispositivo determina que os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, sendo que tais dados devem ser excluídos (i) tão logo atingida a finalidade de seu uso; ou (ii) se encerrado o prazo determinado por obrigação legal - que para o provedores de aplicações é de 6 meses, conforme artigo 15 do Marco Civil da Internet. Tudo isso para garantir a segurança dos dados obtidos dos usuários, bem como o direito à privacidade.

Esse tratamento é importante pois os dados possuem alto valor no mundo virtual, na medida em que, quanto mais dados se obtém, mais se sabe sobre aquele indivíduo, o que viabiliza a entrega de serviços e produtos com maior receptividade no mercado. Por exemplo, se eu curto fotos de carros, a plataforma poderá incluir uma quantidade maior de propagandas de veículos no meu *feed*, pois entenderá que eu gosto de consumir conteúdos que envolvem carros ou estou procurando um para comprar.

A partir disso, os provedores de aplicações de internet adquirem um perfil completo sobre o usuário, tendo conhecimento do que ele gosta, do que ele não gosta, quais são as

---

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;

[14] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. § 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação. § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014 , os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos: I - tão logo atingida a finalidade de seu uso; ou II - se encerrado o prazo determinado por obrigação legal.

pessoas que possuem princípios e ideias parecidas com as dele, quais são as que não tem, entre outros. Por isso, se os dados não forem tratados da forma legal, o princípio da privacidade e da proteção aos dados pessoais serão violados e as informações poderão ser roubadas, vendidas, coletadas ou analisadas por terceiros.

No Brasil, há alguns casos de vazamento de dados que foram extremamente midiáticos, como o caso do Banco Central que, em janeiro de 2022, comunicou um vazamento de dados pessoais vinculados a chaves PIX que estavam sendo guardados pela empresa Acesso Soluções de Pagamento. Dentre os dados vazados, haviam informações como nome completo, CPF, instituição bancária, número de agência e conta.

Para Damásio de Jesus:

> "A proteção à privacidade, item muito agredido na era da tecnologia da informação, também passa a ser um princípio, previsto no inciso II do art. 3º do Marco Civil, assim como a proteção aos dados pessoais, prevista no inc. III do precitado artigo. Ao proteger a privacidade, o Marco Civil põe a salvo toda e qualquer informação textual ou audiovisual que seja considerada privada. Além de proteger a privacidade em geral, o Marco Civil dá ênfase à proteção dos dados pessoais, informações que podem identificar uma pessoa e que comumente são utilizadas ou requeridas pelos provedores de acesso à internet ou provedores de serviços no Brasil. Até hoje, não se dispunha de uma legislação que protegesse o cidadão em face da violação de sua privacidade ou dados pessoais. Com o Marco Civil, empresas ou prestadores poderão ser responsabilizados. Destaca-se que a proteção aos dados pessoais poderá ser regulamentada por lei, que, entendemos, pode ser o Anteprojeto de Proteção de Dados Pessoais, em fase de consulta pública no Brasil"[15].

Nas palavras de Carlos Affonso Souza, Ronaldo Lemos e Celina Bottino:

> "Não existe pleno exercício do direito de acesso à Internet sem a garantia do direito à privacidade. Essa determinação, constante do artigo oitavo do Marco Civil da Internet, serve de guia para que se compreenda a importância da tutela da privacidade para o desenvolvimento da personalidade, para o exercício da cidadania e a sua fruição completa das possibilidades criadas pela comunicação da na rede"[16].

Diante de todo o exposto, verifica-se que o Marco Civil da Internet, legislação que regula a utilização da internet no Brasil, possui como princípios primordiais a privacidade e a proteção de dados pessoais. Isso significa que, durante todo o armazenamento e tratamento dos dados, os provedores de aplicações e conexão devem ser guiados pela privacidade e pela proteção dos dados pessoais, não podendo, em momento algum, fornecer ou deixar com que

[15] Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014, p. 21-22.
[16] Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017, p. 19.

tais dados sejam vazados, sob pena de violar direitos garantidos constitucionalmente aos indivíduos.

2. DADOS QUE OS PROVEDORES DE APLICAÇÕES DE INTERNET ESTÃO OBRIGADOS A ARMAZENAR E/OU FORNECER

2.1 REGISTROS DE ACESSO

Conforme mencionado nos capítulos anteriores, os provedores de aplicações de internet armazenam dados de milhares de seus usuários. No entanto, há certos dados que eles estão obrigados a armazenar e fornecer em caso de ordem judicial. É o caso dos registros de acesso a aplicações de internet, que consistem no número de IP e nos registros de data e hora de acessos dos usuários.

O que se quer deixar claro, inicialmente, é que os provedores de aplicações de internet podem armazenar dados como nome, e-mail, cpf, endereço, entre outros, mas eles só estão **legalmente obrigados** a armazenar os registros de acesso. É isso que dispõe o *caput* do artigo 15 do Marco Civil da Internet:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos **deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento**. (grifos meus)

Com isso, é possível verificar que o Marco Civil da Internet exige aos provedores de aplicações de internet **apenas e tão somente a guarda dos registros de acesso**, assim definidos em seu artigo 5º, inciso VIII, como "*o conjunto de informações referentes à data e hora de uso de uma determinada aplicação a partir de um determinado endereço de IP*", pelo prazo de 6 (seis) meses.

Da leitura integral do Marco Civil da Internet, verifica-se que não há uma menção sequer que impute aos provedores de aplicações de internet o dever de armazenamento, produção de relatórios ou pesquisa e fornecimento de dados de qualquer outra natureza que não os registros de acesso. Dessa forma, os únicos dados que os provedores estão obrigados a armazenar e fornecer são: número de IP e a data e hora de acessos. Qualquer outro dado que não os registros de acesso pode ser inviável de ser produzido e/ou fornecido. Inclusive, assim entende a doutrina:

> "Importante observar, ainda, que os registros de conexão e de acesso à aplicação são as únicas informações obrigatórias de guarda exigidas pelo Marco Civil da Internet, estando tais provedores desobrigados de guardar quaisquer outros dados pessoais, cadastrais ou comunicações. A guarda dos registros possui relevância para a identificação de usuários responsáveis por ilícitos civis ou penais, considerada a vedação ao anonimato prevista no artigo 5º, IV CRFB/88"[17].

Reitera-se: pode até ser que os provedores detenham determinados dados que não os registros de acesso, como os dados cadastrais (nome, endereço, CPF, e-mail), mas é evidente que a lei só obriga os provedores a armazenarem e fornecerem os registros de acesso. Para Carlos Affonso Souza, Ronaldo Lemos e Celina Bottino, isso possui uma razão de ser:

> "Até mesmo como uma decorrência do princípio da minimização de dados, a preservação de dados para além do mandamento legal deve ser vista sempre à luz dos limites concedidos ao tratamento de dados pela empresa e a utilidade desses dados para empresas e autoridades investigativas. Provedores devem evitar a guarda de dados pessoais desnecessários para o exercício de sua atividade, sendo certo que o artigo 16, II, do Marco Civil da Internet veda expressamente a guarda "de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular". Da mesma forma, o artigo 13, §2º do Decreto 8771/16 determina aos provedores a retenção da menor quantidade possível de dados de seus usuários. **Além disso, não há qualquer obrigação por lei de dados pessoais para além de registros de conexão e registros de acesso a aplicações**"[18]. (grifos meus)

Assim, a obrigação de armazenar **apenas** registros de acesso é motivada pela diminuição nos riscos de violação ao direito à privacidade e à proteção de dados pessoais. Conforme visto, o parágrafo 2º do art. 13 do Decreto 8.771/2016 determina que os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, para garantir a segurança dos dados obtidos dos usuários, bem como o direito à privacidade.

Ora, quanto mais dados o provedor de aplicações de internet for **obrigado** a armazenar, maiores serão os cuidados com o tratamento de tais dados, mas também maiores serão os riscos de haver falhas em tal tratamento. A título de exemplo, um gado composto por 10 vacas é muito mais fácil de ser controlado e tratado do que um gado composto por 10 mil vacas, que é o que ocorre *in casu*: o tratamento de 100 mil dados possui menos riscos de violação do que um tratamento de 100 bilhões de dados.

Como visto, os registros de acesso são compostos por número de IP e data e hora de acesso. Para facilitar a compreensão, pontua-se que o número de IP é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local. O termo "IP" vem do inglês

[17] Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017, p. 45.
[18] Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017, p. 25.

"Internet Protocol" que consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local. Além disso, as datas e horas de acesso nada mais são do que os registros do momento (dia e hora) que o usuário, através daquele número de IP, acessou o ambiente proporcionado pelo provedor de aplicações de internet.

2.2 SUFICIÊNCIA DO REGISTROS DE ACESSO PARA IDENTIFICAÇÃO DE USUÁRIOS

Muito se diz, em debates judiciais, que o fornecimento dos registros de acesso não é suficiente para identificar o usuário e que seria necessário fornecer dados cadastrais (como e-mail, nome, CPF, endereço) para identificar determinada pessoa - o que foge à regra do artigo 15 do Marco Civil da Internet, já que a legislação não obriga os provedores a armazenam dados que não sejam os registros de acesso.

No entanto, é evidente que o fornecimento dos registros de acesso é suficiente para identificar determinado usuário pois, com o IP em mãos, a parte poderá verificar, por conta própria, através de sites na internet, quem é o provedor de conexão daquele IP, podendo requerer ao provedor de conexão os dados que ele possui daquele usuário.

Para facilitar a visualização, vamos supor que o Facebook Brasil, através do provedor Meta Platforms Inc., forneça registros de acesso de determinado usuário em um caso judicial. Através de tais dados, o Autor poderá verificar, por conta própria, através de sites na internet, quem são os provedores de conexão daquele IP, ou seja, quem é o responsável por fornecer serviços de conexão à Internet para aquele usuário, como a Vivo, a Claro, a Oi, no Brasil. Com essa informação em mãos, o Autor poderá requerer a expedição de ofícios aos provedores de conexão, os quais poderão identificar o usuário através do fornecimento de seus dados.

Assim, conclui-se que os registros de acesso são suficientes para a identificação do usuário. Aliás, assim já decidiu o Egrégio Superior Tribunal de Justiça e os tribunais pátrios:

> “Portanto, espera-se que o provedor adote providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para permitir a identificação dos usuários de determinada aplicação de internet. (...) **Dessa forma, esta Corte entende como suficiente a apresentação dos registros de número IP**. (...) Esse entendimento é corroborado por diversos precedentes da Terceira e Quarta Turmas desta Corte Superior, como o REsp 1.308.830/RS (Terceira Turma, julgado em 08/05/2012, DJe 19/06/2012), o REsp 1.512.647/MG (Segunda Seção, julgado em 13/05/2015, DJe 05/08/2015), o AgRg no REsp 1.384.340/DF (Terceira Turma, julgado em 05/05/2015, DJe 12/05/2015) e o AgRg no REsp 1402104/RJ (Quarta Turma, julgado em 27/05/2014, DJe 18/06/2014) (...) **Pelo exposto acima,**

percebe-se que a jurisprudência deste Superior Tribunal de Justiça é consolidada no sentido de – para adimplir sua obrigação de identificar usuários que eventualmente publiquem conteúdos considerados ofensivos por terceiros – é suficiente o fornecimento do número IP correspondente à publicação ofensiva indicada pela parte. (...) Os endereços IPs, ressalte-se, são essenciais na arquitetura da internet, que permite a bilhões de pessoas e dispositivos se conectarem à rede, permitindo que trocas de volumes gigantescos de dados sejam operadas com sucesso. Nesses termos, a doutrina define que "o endereço IP (internet protocol) é a cédula de identidade de cada terminal, somente sendo admitido um terminal para cada número IP disponível, de modo que seja impossível a conexão de dois dispositivos à rede com o mesmo número, o que gera conflitos na transmissão e recepção de dados e, comumente, faz com que a própria rede derrube o acesso de todos os dispositivos com números colidentes". (HAIKAL, V.A. Da significação jurídica dos conceitos integrantes do art. 5º. In: LEITE, G.S.; LEMOS, R. (Coords.). Marco Civil da Internet. São Paulo: Atlas, 2014, p. 320). (...) **É certo que a limitação dos dados a serem obrigatoriamente guardados pelos provedores de aplicações de internet tem uma razão de ser, que é a tutela jurídica da intimidade e da privacidade, consagrada no art. 5º, inciso X, da Constituição Federal de 1988, foi expressamente encampada pelo Marco Civil da Internet, que assegura como direitos dos usuários da rede a proteção à privacidade** (...) Para concluir essa discussão, apesar de não envolvido diretamente na solução desta controvérsia, é interessante notar que o decreto que regulamenta o Marco Civil da Internet (Decreto nº 8.771/2016) dispõe em seu art. 11 que, realizada a requisição de dados pela autoridade administrativa competente, o provedor que não coletar dados cadastrais deverá fazer saber a inexistência de tais informações à autoridade, ficando desobrigado a fornecê-los (...) **Além disso, no art. 13, § 2º, do Decreto nº 8.771/2016 também fica estabelecido que os provedores de aplicações de internet "devem reter a menor quantidade possível de dados pessoais", o que reforça a inexigibilidade jurídica do armazenamento e fornecimento de dados que não sejam os registros de acesso, expressamente apontados pelo Marco Civil da Internet como os únicos que os provedores de aplicações devem guardar e, eventualmente, fornecer em juízo**. (...) Forte nessas razões, CONHEÇO e DOU PROVIMENTO ao recurso especial, com fundamento no art. 255, § 4º, III, do RISTJ, para **afastar a obrigação determinada pelo Tribunal de origem de fornecimento das informações extravagantes aos registros de acesso de aplicações, nos termos do art. 5º, VIII, do MCI**"[19]. (grifos meus)

"O apelante questiona a legalidade do fornecimento dessas informações, aduzindo que a obrigação imposta por lei é o fornecimento apenas dos registros de acesso a aplicações da internet. E com razão, **não podendo a ré ser instada a fornecer informação que não possui**. Isso porque, para que se abra uma conta nas redes sociais Facebook e Instagram, basta o fornecimento de uma conta de e-mail e de telefone. São essas as informações necessárias e que foram armazenadas pelo réu, as quais, por ordem judicial, foram fornecidas à parte autora, além dos endereços de IP e data/horários de acesso. **Não consta, porém, que o Facebook esteja de posse das informações determinadas na r. sentença (nome, endereço, RG e CPF do usuário), e nem a lei a obriga seu armazenamento**. (...) Destarte, conforme o entendimento do Colendo STJ, **não há obrigação pelo apelante Facebook, provedor de serviços de aplicação, que disponibiliza um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet (art. 5º, VII, Lei n. 12.965/2014), de fornecer dados consistentes em localização geográfica (coordenadas de GPS), nome, RG, CPF, e-mail, data de nascimento, endereço, número de telefone, por não serem de coleta obrigatória quando do cadastramento do usuário, suprindo o dever de identificação dos usuários o fornecimento do número de protocolo na internet (IP) dos computadores utilizados para o cadastramento de cada conta** (REsp

[19] REsp n. 1.829.821/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 25/8/2020, DJe de 31/8/2020

> 1342640/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 07/02/2017, DJe 14/02/2017)"[20] (grifos meus)
>
> "Com efeito, tem-se que a autora não pretende a obtenção dos dados de acesso ao aplicativo, mas, sim, os dados pessoais dos titulares da conta vinculada ao número telefônico. (...) Contudo, nota-se que **a ré não tem obrigação de coletar e guardar dados pessoais de seus usuários**, o que se extrai do art. 15, "caput" e §3º da Lei 12.965/2014"[21] (grifos meus)
>
> "**A obrigatoriedade de informações, em conformidade com o art. 22 da Lei n. 12.965/2015, cinge-se aos registros de conexão ou de registros de acesso a aplicações de Internet**. Registro de acesso, por sua vez, nos termos do art. 5º, VIII, da Lei 12.965/2015, compreende tão somente "o conjunto de informações referentes à data e hora de uso de uma determinada aplicações de Internet a partir de um determinado endereço IP". **Portanto, não constitui obrigação do provedor de conteúdo o armazenamento e muito menos o fornecimento da qualificação completa de seus usuários. Informações como nome e endereço dos usuários deverão ser obtidas perante o provedor de conexão, mediante a informação do IP do usuário**, afastando-se a cominação da da multa na parte do título judicial que determinou obrigação de cumprimento impossível pela requerida"[22]. (grifos nossos)

Diante de todo o exposto, verifica-se que o Marco Civil da Internet, em seu artigo 15, obriga os provedores de aplicações de internet a armazenarem **apenas** registros de acesso, o que inclui o endereço de IP e a data e hora do acesso, nos termos do artigo 5º, inciso VIII da legislação. Nesse sentido, os provedores até podem manter dados que não os registros de acesso, mas é evidente que somente estão obrigados a armazenar e fornecer os registros.

Por fim, pontua-se que, conforme reconhecido pela jurisprudência pátria, o fornecimento do IP e da data e hora de acesso são suficientes para a identificação do usuário, não havendo motivos para o fornecimento de dados extravagantes.

2.3 PRAZO LEGAL DE ARMAZENAMENTO DOS REGISTROS DE ACESSO

Além de limitar a obrigação de dados aos registros de acesso, o artigo 15 do MCI também limita o tempo em que esses dados devem permanecer armazenados pelo provedor de aplicação. Conforme depreende-se da parte final do *caput* do dispositivo, os registros de acesso devem ser mantidos pelo prazo de 6 (seis) meses, a partir da criação da conta, tudo em prol da segurança dos dados:

---

[20] TJ-SP - AC: 10844340320178260100 SP 1084434-03.2017.8.26.0100, Relator: Clara Maria Araújo Xavier, Data de Julgamento: 18/08/2021, 8ª Câmara de Direito Privado, Data de Publicação: 19/08/2021
[21] TJ-SP - AC: 10036451420188260704 SP 1003645-14.2018.8.26.0704, Relator: Angela Lopes, Data de Julgamento: 25/08/2020, 9ª Câmara de Direito Privado, Data de Publicação: 26/08/2020
[22] TJSP, 1º Câmara de Direito Privado, Agravo de Instrumento 2177435-68.2016.8.26.0000, rel. Des. Alcides Leopoldo e Silva Junior, j. 22.11.2016, Dje 23.11.2016

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, **pelo prazo de 6 (seis) meses**, nos termos do regulamento. (grifos nossos)

O parágrafo segundo do dispositivo dispõe que esse prazo de armazenamento poderá ser superior a 6 (seis) meses, desde que tal solicitação seja feita por autoridade policial ou administrativa ou pelo Ministério Público. Assim, o parágrafo 2º trata-se de exceção à regra, que é de 06 (seis) meses. Isso, inclusive, é reconhecido pela doutrina:

> "Ainda, a Lei estipula o prazo durante o qual esses registros devem ser guardados pelos provedores do serviço, que é de um ano para os provedores de conexão (artigo 13 da Lei nº 12.965), os quais não podem repassar tal obrigação a terceiros; bem como de seis meses para os provedores de acesso a aplicações que exerçam atividade organizada, profissionalmente e com fins econômicos (artigo 15 da Lei nº 12.965)"[23].

> "Estes provedores deverão guardar os registros de acesso às aplicações pelo prazo de 6 (seis) meses, prazo este contado do evento que gerou os registros. Importa dizer que a obrigação vale apenas para provedores que exerçam essa atividade de forma organizada, profissionalmente e com fins econômicos[24]".

É evidente que, assim como a norma limita os dados a serem armazenados em prol da segurança de tais dados, a limitação do período de armazenamento ocorre com o mesmo propósito. Isso porque, os riscos de violação à privacidade e à proteção aos dados pessoais aumentam quando você armazena os dados por mais tempo. Aliás, é justamente o que propõe o artigo 13, parágrafo 2º, inciso II do Decreto Lei 8.771/2016 cumulado com o artigo 15 do Marco Civil da Internet, ao limitarem a retenção dos dados pelo prazo de 6 (seis) meses.

A jurisprudência também caminha no mesmo sentido:

> "**Como forma de conferir efetiva proteção, especificamente, aos registros de acesso a aplicações e, assim, minimizar a restrição à garantia da intimidade e proteção dos dados, o art. 15 da Lei 12.965/2014 determina que eles sejam armazenados pelo período de apenas 06 (seis) meses**. Esse prazo tem como termo inicial o "evento que gerou os registros" (JESUS, Damásio de. Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014. E-book. São Paulo: SARAIVA, 2014). (...) **Apesar da reconhecida importância que a preservação desses registros assume na identificação da autoria de ilícitos praticados na internet, a definição de um prazo de guarda demonstra a preocupação do**

[23] Marco Civil da Internet. São Paulo: Atlas, 2014. p. 154.
[24] Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014, p. 59.

> **legislador em proteger a intimidade do usuário e assegurar o sigilo dos dados**"[25]. (grifos meus)
>
> "(...) Assim, a alegação da autora de cumprimento parcial da obrigação não prospera, tendo em vista que o artigo 15 da Lei 12.965/2014 (Marco Civil da Internet) prevê o prazo de seis meses para a guarda dos dados, não havendo obrigatoriedade de armazenamento por prazo superior ao estabelecido no citado artigo, não havendo que se falar em conversão em perdas e danos"[26].
>
> "Não obstante tal dever, a lei é categórica ao determinar esse armazenamento por prazo determinado, qual seja, 06 (seis) meses, de modo que, esse lapso temporal é relativo aos meses anteriores à intimação judicial para cumprir a determinação de fornecimento dos IP's"[27].
>
> "Nos termos da Lei 12.965/2014, artigo 15, "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento". No caso, há informação de que o perfil https://www.facebook.com/joãodoscarros já se encontrava excluído na data de 19/11/2020, conforme indicado pelo magistrado quando analisou a tutela de urgência (mov. 9.1). De outra parte, a ordem recebida de quebra de sigilo dos dados só a ser perfectibilizada com o julgamento dos embargos de declaração, do qual a ré foi intimada em 28/06/2021 (mov. 59.0). **Desse modo, excluída a conta pelo usuário e, passados mais de 06 (seis) meses daquela data, não tem mais como o fornecedor fornecer os dados do perfil "João dos Carros"**[28]. (grifos meus)

Com isso, finaliza-se o presente capítulo partindo das seguintes premissas: (i) o provedor de aplicações de internet está obrigado somente a armazenar e fornecer registros de acesso, o que inclui endereço de IP e data e hora de acesso; (ii) o fornecimento de IP no procedimento judicial é suficiente para a identificação do usuário, conforme reconhecido pela jurisprudência pátria; e (iii) os registros de acesso devem ser armazenados pelos provedores de aplicações pelo prazo de seis meses, a contar da data da criação da conta, salvo se for requerido por autoridade policial ou administrativa ou pelo Ministério Público a ampliação de tal prazo. Dito isso, passar-se-á a analisar as condições necessárias para que os registros de acesso sejam fornecidos em um procedimento judicial.

---

[25] REsp n. 1.850.875/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 23/2/2021, DJe de 1/3/2021

[26] TJ-SP, Apelação Cível nº 1005138-34.2019.8.26.0011, Des. Rel. Alexandre Marcondes, 6ª Câmara de Direito Privado, j. 27/05/2021

[27] TJ-GO - Apelação (CPC): 04132935820148090097, Relator: Gustavo Dalul Faria, Data de Julgamento: 23/05/2019, 1ª Câmara Cível, Data de Publicação: DJ de 23/05/2019

[28] TJ-PR - RI: 00021558120208160186 Ampére 0002155-81.2020.8.16.0186 (Acórdão), Relator: Maria Fernanda Scheidemantel Nogara Ferreira da Costa, Data de Julgamento: 13/12/2021, 1ª Turma Recursal, Data de Publicação: 14/12/2021

3. O ARTIGO 22 DO MARCO CIVIL DA INTERNET: REQUISITOS LEGAIS PARA O FORNECIMENTO DE DADOS PELO PROVEDOR

3.1 ORDEM JUDICIAL, ATO ILÍCITO, JUSTIFICATIVA E PERÍODO

Como visto nos capítulos *an passant*, os dados dos usuários que contratam com os provedores de aplicações de internet são protegidos por sigilo, nos termos dos artigos 5º, incisos X e XII, da Constituição Federal, artigo 7º, inciso III, artigo 10º, parágrafo 1º e artigo 15, parágrafo 3º do Marco Civil da Internet.

Assim, de acordo com o ordenamento legal vigente, para que seja possível fornecer os dados atinentes a usuários da internet é imprescindível que haja prévia ordem judicial determinando a disponibilização desses dados, bem como que a parte requerente apresente (i) fundados indícios da ocorrência do ilícito; (ii) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e (iii) período ao qual se referem os registros. É o que dispõe o artigo 22, *caput* e parágrafo único do Marco Civil da Internet, *in verbis*:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. **Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade**:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros. (grifos nossos)

Caso todos os requisitos previstos no parágrafo único do dispositivo acima não estejam presentes, o pedido de fornecimento de dados será inadmissível. Vale pontuar, ainda, que tais requisitos são cumulativos e, por isso, todos eles devem estar garantidos no momento da solicitação dos dados, o que fica cristalino pela sua própria redação.

Assim, é necessária justificativa motivada dos dados solicitados para fins de investigação ou instrução probatória, mas também é imprescindível a comprovação de fundados indícios de ilícitos cometidos pelo usuário, bem como o período ao qual se referem os registros. Inclusive, a jurisprudência do Colendo Superior Tribunal de Justiça e de tribunais pátrios reconhece a cumulatividade dos requisitos previstos no artigo 22, parágrafo único do Marco Civil da Internet:

> "Para que seja possível ao juiz determinar o fornecimento desses dados, é necessário que, além dos requisitos exigidos pela legislação processual (e.g. legitimidade da parte), estejam satisfeitos os pressupostos elencados no art. 22 do Marco Civil da Internet, a saber: (i) fundados indícios da ocorrência do ato ilícito; (ii) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e (iii) período ao qual se referem os registros. Inegavelmente, trata-se de mais uma garantia de privacidade conferida pelo Marco Civil da Internet aos usuários de aplicações, ao afirmar que seus registros de acesso apenas serão disponibilizados na presença de atos ilícitos. (...) **Portanto, caso ausente <u>quaisquer</u> desses requisitos, o pedido de fornecimento de registros de acesso a aplicações deverá ser indeferido**"[29]. (grifos meus)

> "Compulsando os autos originários, observa-se que, no caso em tela, o agravante requer a quebra do sigilo de dados telemáticos, a fim de obter informações da procedência e dos dados pessoais do titular do *e-mail* utilizado para lhe imputar calúnias, as quais o agravante afirma serem inverídicas e consequentemente, vão de encontro a sua reputação, honra e dignidade. Ademais, o agravante alega que tais informações serão necessárias para a persecução investigatória, mormente para formar o conjunto probatório em processo judicial para a responsabilização cível dos envolvidos. **Contudo, com base no art. 22 do Marco Civil da Internet (Lei nº 12.965/2014), o requerimento para o fornecimento dos registros de conexão ou de registros de acesso a aplicações da internet, deverá conter os seguintes requisitos <u>cumulativos</u>**: "Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros"[30]. (grifos meus)

> "Quanto ao mérito, verifica-se que a celeuma jurídica posta nos autos diz respeito à obrigação da ré, responsável pelo serviço "Gmail", em fornecer os dados sobre o IP, dados cadastrais e porta de origem do autor da mensagem eletrônica (e-mail) acostada às fls. 10/11. **Vê-se, então, que para que seja possível o acolhimento do pleito da exordial, mister se faz o preenchimento dos requisitos previstos no art. 22 da Lei de Regência**. (...) No caso dos autos, nota-se justamente a ausência do requisito previsto no inciso I do art. 22, na medida em que a mensagem contida às fls. 10/11 não se consubstancia em qualquer ilícito civil ou penal. O conteúdo da mensagem não se mostra desrespeitoso, mas apresenta um mero tom de crítica, acobertado este pelo direito constitucional da liberdade de expressão (art. 5º, IV e IX da CF e também pelo Marco Civil da Internet (art. 3º, I)"[31]. (grifos meus).

Sobre o tema, leciona a doutrina:

> "O Marco Civil prevê a possibilidade de o interessado requerer judicialmente informações sobre os registros na internet com o fim de formar provas em processo

[29] REsp n. 1.850.875/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 23/2/2021, DJe de 1/3/2021

[30] TJ-DF 07424922820228070000 1695735, Relator: LUCIMEIRE MARIA DA SILVA, Data de Julgamento: 27/04/2023, 4ª Turma Cível, Data de Publicação: 12/05/2023

[31] TJSP, 2ª Vara de Juizado Especial Cìvel, Ação Cìvel 1006845-27.2016.8.26.0016, Juiz Leonardo Fernandes dos Santos, j. 13.12.2016, DJe 19.12.2016

> judicial. Essa requisição judicial pode ser feita no curso de um processo de forma incidental ou em processo autônomo, devendo ser requerido ao juiz que ordene ao titular do provedor, responsável pela guarda, o fornecimento de registros de conexão ou de registros de acesso a aplicações (conteúdos) de internet. (...) Sempre respeitando outros requisitos previstos em lei, o requerimento judicial deverá conter: os fundados indícios da ocorrência do ilícito; a justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e o período ao qual se referem os registros. **O desrespeito a esses requisitos implicará na inadmissibilidade da requisição**"[32]. (grifos meus)

> "**O Marco Civil estipula que os requerentes têm de atender a <u>todos</u> os requisitos legais para o ingresso da ação judicial**, tal como aqueles insertos no art. 319 e ss. do CPC, em termos de condições da ação e pressupostos processuais (...). Além desses, o Marco Civil reforça que o requerente dos pedidos tenha: fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e período ao qual referem os registros"[33]. (grifos meus)

Diante do exposto, fica claro que o fornecimento de dados do usuário pelo provedor de aplicações deve se dar somente mediante ordem judicial. No entanto, tal ordem só poderá ser proferida se a parte requerente, ao formular o pedido, apresentar fundados indícios de ocorrência de ato ilícito cometido pelo usuário cujos dados se requer; apresentar justificativa motivada da utilidade dos registros; e, dizer o período ao qual se referem os registros.

A corroborar com tal tese, insta mencionar que o artigo 11, parágrafo 2º do Decreto nº 8.771/2016[34], que regulamentou o Marco Civil da Internet, veda ordens genéricas de quebra de sigilo de dados, devendo estar presentes todos os requisitos autorizadores do parágrafo único do artigo 22 do Marco Civil da Internet, para que o Poder Judiciário possa ordenar a quebra dos dados de determinado usuário.

Assim, a necessidade de ordem judicial possui como fundamentação a proteção ao sigilo dos dados dos usuários. O fato de uma pessoa ter que fazer um requerimento ao juízo, que irá analisar o pedido e deferir ou indeferi-lo, faz com que o sigilo seja resguardado e garante que os dados só sejam fornecidos se, de fato, os requisitos do artigo 22 do Marco Civil da Internet estiverem preenchidos - o que deve ser analisado e atestado pelo Juízo.

Nesse sentido:

> "**A norma do art. 10 cuida da guarda e disponibilização dos registros de conexão e de acesso a aplicações de Internet bem como de dados pessoais e do conteúdo de comunicações privadas, estipulando que estes devem atender à**

---

[32] Marco Civil da Internet comentado. 1. ed. São Paulo: Atlas, 2017. p. 115-116.
[33] Marco Civil da Internet comentado. 1. ed. São Paulo: Atlas, 2017.p. 162.
[34] Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais. (...) § 3o Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

> **preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, somente podendo ser disponibilizados mediante ordem judicial**, ou, na hipótese de dados cadastrais que informem qualificação pessoal, filiação e endereço, a autoridades administrativas que detenham competÊncia legal para a sua requisição"[35]. (grifos meus).

Para deixar mais claro, vale trazer alguns conceitos doutrinários que abordam os requisitos presentes no parágrafo único do artigo 22 do Marco Civil da Internet:

> "a)Fundados indícios da ocorrência do ilícito:
> A demonstração desse requisito pode se dar, por exemplo, com o uso da ata notarial para comprovar um crime de difamação, um uso indevido de imagem, marca ou material intelectual protegido. Ainda, caso se trate de uma requisição para identificar a origem de um ataque a determinado computador a utilização de um laudo pericial atestando o ilícito é suficiente. Veja, que sem a demonstração do ilícito não se justifica a quebra do sigilo e a violação da privacidade, princípio bastante evidenciado no Marco Civil.
>
> b)Justificativa motivada da utilidade dos registros:
> A utilidade dos registros é fundamental para a requisição ser deferida. Caso o magistrado não identifique que os registros a serem fornecidos poderão ser úteis para fins de investigação ou instrução probatória, o indeferimento é medida que se impõe. Como no requisito anterior, a utilidade da requisição também previne contra atos de violação à intimidade e à vida privada. Evitando com o pretexto de investigação de um ilícito se obtenha mais informações do que aquelas efetivamente necessárias.
>
> c)Período ao qual se referem os registros:
> O terceiro requisito imposto pelo parágrafo único do artigo 22 é a obrigatoriedade de o pedido conter o período ao qual se referem os registros, para assim poder confrontar a utilidade dos mesmos, impedindo, mais uma vez o acesso indevido e despropositado, bem como permitir um cumprimento pelo provedor de forma efetiva. Como nos pedidos de remoção (§ 1º, art. 19), a indicação precisa é fundamental para que a ordem seja cumprida"[36].

Com isso, é possível verificar que, para requerer os dados de determinado usuário, a parte requerente deverá demonstrar, em seu pedido, que o usuário cujos dados se quer obter cometeu ato ilícito ao usar o serviço disponibilizado pelo provedor de aplicações de internet. A título de exemplo, se um indivíduo faz um post ameaçador contra o requerente, é isso que o requerente deverá demonstrar ao juízo: o usuário, através do serviço disponibilizado pelo provedor de aplicações, cometeu ato ilícito ao publicar conteúdo ameaçador ao requerente.

Mas não é só. Conforme antecipado, o requerente também deverá justificar a utilidade na obtenção dos registros, isto é, deverá demonstrar que, através da obtenção dos registros de acesso, será possível proceder com investigação ou instrução probatória em determinado caso.

---

[35] TJSP, 9ª Câmara de Direito Privado, Apelação Cível 1110702-65.2015.8.26.0100, rel. Des. Angela Lopes, j. 30.05.2017, DJe 31.05.2017

[36] A requisição judicial de registros de conexão e aplicações no Marco Civil. In: Direito & Internet III: Marco Civil da Internet. São Paulo: Quartier Latin, 2015, p. 491-492.

Caso não haja utilidade na obtenção dos dados, o requerimento será inadmissível, sob pena de se violar o sigilo dos dados.

Por fim, é necessário que a parte também indique o período ao qual se referem os registros. Isso é importante para que o juízo complete a análise sobre o pedido, aferindo se os os períodos cujos dados se requer são compatíveis com a realidade fática do caso.

Com isso, conclui-se que, como os dados dos usuários fornecidos aos provedores de aplicações de internet são sigilosos, é necessário que, para que tal sigilo seja quebrado, haja: (i) ordem judicial nesse sentido; e (ii) requerimento que contenha fundados indícios de ocorrência de ato ilícito; justificativa motivada da utilidade dos registros; e, o período ao qual se referem os registros requeridos.

3.2 A IMPORTÂNCIA DA COMPROVAÇÃO DO ATO ILÍCITO, SOB PENA DE VIOLAÇÃO AO ART. 22 E AO DIREITO DE PRIVACIDADE DO USUÁRIO

Conforme visto, o legislador deixa claro, na disposição do artigo 22 do Marco Civil da Internet, a possibilidade de quebra sobre o sigilo de dados dos usuários de aplicações de internet, desde que determinados requisitos estejam presentes.

Dentre os requisitos existentes, há menção expressa à necessidade de existência de "fundados indícios de ocorrência de ilícito", o que deve ser objeto de efetiva apreciação na decisão judicial. A propósito, assim entende a jurisprudência do Colendo Superior Tribunal de Justiça:

> "Assim, qualquer indivíduo que tenha sido lesado por ato praticado via internet poderá demandar o provedor respectivo para obter os referidos dados. **Para que seja possível ao juiz determinar o fornecimento desses registros, no entanto, é necessário que, além dos requisitos exigidos pela legislação processual (p. ex. legitimidade da parte), estejam satisfeitos os pressupostos elencados no parágrafo único do art. 22 do Marco Civil da Internet**, a saber: a) fundados indícios da ocorrência do ato ilícito; b) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e c) período ao qual se referem os registros"[37]. (grifos meus)

> "Diante disso, ainda que muitos busquem na web o anonimato, este não pode ser pleno e irrestrito. A existência de meios que possibilitem a identificação de cada usuário se coloca como um ônus social, a ser suportado por todos nós objetivando preservar a integridade e o destino da própria rede. Isso não significa colocar em risco a privacidade dos usuários. Os dados pessoais fornecidos ao provedor devem

[37] REsp n. 1.961.480/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 7/12/2021, DJe de 13/12/2021

> ser mantidos em absoluto sigilo – tal como já ocorre nas hipóteses em que se estabelece uma relação sinalagmática via Internet, na qual se fornece nome completo, números de documentos pessoais, endereço, número de cartão de crédito, entre outros – **sendo divulgados apenas quando se constatar a prática de algum ilícito e mediante ordem judicial**"[38]. (grifos meus)

Em outras palavras, o requerente deverá comprovar que o usuário cometeu algum ato ilícito ao usufruir o serviço fornecido pelo provedor de aplicações, como, por exemplo, a publicação de um conteúdo ameaçador, ofensivo ou que vá de encontro à legislação brasileira.

Assim, aqueles que não cometem o ato ilícito, não devem ter o seu sigilo de dados quebrado, sob pena de se violar a proteção aos dados pessoais do usuário. Isso porque o Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, tem por objeto a proteção das garantias à intimidade e privacidade dos usuários no âmbito da internet (artigos 3º, incisos II e III; 7º, inciso I; 8º, *caput*; 10, do MCI), premissas essas que já estão asseguradas na Magna Carta (artigo 5º, inciso X, Constituição Federal).

O que se vê corriqueiramente, são litigantes que requerem o fornecimento de dados de usuários cujo ato ilícito cometido não foi comprovado. Por exemplo, suponha-se que "A" realiza um post ofensivo à "B" em um grupo que é administrado por "C" e, por isso, "B" requer o fornecimento dos dados de "A", que cometeu o ilícito, e de "B", que nada fez, mas é o administrador do grupo. Nesse caso, se os dados de "B" forem fornecidos, seu direito à privacidade será violado sem justa causa, já que o ato ilícito não restou comprovado. Ora, não há ilicitude em ser mero administrador de um grupo.

Em uma outra situação, "D" elabora e publica um conteúdo ofensivo à "F", e "G" curte este conteúdo. Por isso, "F" requer os dados de "D" e de "G". Veja que, nesse caso, o único que cometeu ato ilícito foi "C", ao publicar o conteúdo ofensivo à "D", enquanto "F" não cometeu nenhum ato ilícito. Isso porque, a função "curtir" nas redes sociais pode ter diversos sentidos, como anuir com o que foi dito - o que está dentro da esfera da liberdade de expressão do indivíduo e, por isso, não caracteriza ato ilícito -, ou registrar que aquele conteúdo foi lido pelo usuário que optou por curti-lo.

Assim, é evidente que, sob pena de se violar um direito garantido tanto pelo Marco Civil da Internet, quanto pela Constituição, não se pode quebrar o sigilo de dados de usuários que não cometeram ato ilícito através do serviço fornecido pelos provedores de aplicações.

[38] REsp n. 1.192.208/MG, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 12/6/2012, DJe de 2/8/2012

Ainda, vale ressaltar que o provedor de aplicações não é o responsável por averiguar se há ilicitude no ato, ou não, pois essa análise deverá ser feita pelo judiciário. No entanto, é imprescindível que o requerente, ao formular o pedido de fornecimento dos dados, apresente fundados indícios de ocorrência de ilícito, para que o Juízo tenha mecanismos e provas para averiguar tal ocorrência e, se for o caso, deferir o pedido de fornecimento de dados.

Caso a parte não fundamente os ilícitos em seu pedido, o fornecimento de dados requerido deverá ser indeferido pelo Juízo, como vem reconhecendo a jurisprudência pátria:

> "Embora seja direito do autor proteger a sua honra quando entendê-la ofendida, por outro lado, para o exercício dessa defesa, há a exposição de dados de identificação e informativos de outra pessoa, até então protegidas, em razão da preservação de sua intimidade e vida privada. Também não é demais observar que tais dados servirão para formar conjunto probatório em outro processo judicial, cível ou penal, circunstância ainda mais expositiva, ainda que eventualmente haja segredo de justiça. O art. 22, parágrafo único, da Lei 12.965/2014, justamente elenca as condições necessárias ao deferimento do pedido (...) **Contudo, o fundado indício de ocorrência de ilícito não está presente no caso concreto**. A URL indicada como portadora do conteúdo ofensivo está, aparentemente, indisponível"[39]. (grifos meus)

> "Igualmente não assiste razão à apelante em relação ao pedido de fornecimento de "todas as informações" do usuário anônimo que publicou o "blog". Isso porque **o fornecimento dos dados cadastrais e registros de conexão de usuário apenas se faz cabível diante de fundados indícios da ocorrência de ilícitos civis ou penais, nos termos do art. 22 do Marco Civil da Internet, hipótese não verificada no caso, pois, como já mencionado acima, não houve extrapolação dos limites da liberdade de expressão** (arts. 5º, IV, e 220, §§ 1º e 2º da Constituição Federal e arts. 3º, I, e 8º do Marco Civil da Internet)"[40]. (grifos meus)

> "Assim, **uma vez que não há ilícito nas publicações, inexiste fundamento para quebra do sigilo de dados do usuário, nos termos do art. 22 do Marco Civil da Internet**. (...) Como se vislumbra, **para que o provedor seja obrigado a disponibilizar os dados pessoais do usuário, devem estar preenchidos todos os requisitos previstos nas alíneas I, II e III do parágrafo único, do art. 22, da Lei 12.965/14**. (...) Como se observa, a sentença objurgada reconheceu que as publicações em questão não se mostram ofensivas ou difamatórias, tratando-se apenas de manifestações de insatisfações e/ou descontentamento com o serviço prestado pela autora/recorrida; contra o que não se insurgiu a parte apelada. **Desta feita, inexistindo indícios da ocorrência do ilícito, resta inviabilizado o pedido inicial, no sentido de "disponibilizar os registros com os dados pessoais do criador da comunidade, ou informações que possam contribuir para a identificação do usuário ou do terminal**." Ante o exposto, conheço do recurso de apelação e, rejeitando a preliminar, lhe dou provimento, para o fim de afastar a obrigação imposta ao apelante, no sentido de fornecer os dados pessoais relativos ao

[39] TJSP; Agravo de Instrumento 2249987-26.2019.8.26.0000; Relator (a): Edson Luiz de Queiróz; Órgão Julgador: 9ª Câmara de Direito Privado; Foro de General Salgado - Vara Única; Data do Julgamento: 28/01/2020; Data de Registro: 30/01/2020

[40] TJ/PR - APL: 00045816320168160103 PR 0004581-63.2016.8.16.0103 (Acórdão), Relator: Desembargador Fernando Paulino da Silva Wolff Filho, Data de Julgamento: 23/03/2020, 17ª Câmara Cível, Data de Publicação: 23/03/2020

> usuário criador da conta discutida, junto ao site do requerido/apelante"[41]. (grifos meus)

Diante do exposto, conclui-se que para que o fornecimento de dados seja deferido pelo Juízo, é necessário que o requerente comprove a presença de fundados ilícitos cometidos pelo usuário cujos dados se requer. Caso tal usuário não tenha cometido o ato ilícito, o Juízo deverá inadmitir o pedido, sob pena de se violar o direito de privacidade e de proteção aos dados pessoais, garantidos pelo Marco Civil da Internet e pela Constituição.

[41] TJMS. Apelação Cível n. 0833103-64.2014.8.12.0001, Campo Grande, 1ª Câmara Cível, Relator (a): Desª. Tânia Garcia de Freitas Borges, j: 17/10/2018, p: 18/10/2018

4. A EMENDA CONSTITUCIONAL Nº 115/22 E SEUS IMPACTOS NO FORNECIMENTO DE DADOS PELO PROVEDOR

À luz do exposto, é possível verificar que o armazenamento de dados pelos provedores de aplicações ganhou atenção a partir da utilização em massa das redes sociais. No entanto, a fim de vedar o anonimato na internet, o Marco Civil da Internet estabelece que os usuários podem ter os seus dados compartilhados mediante ordem judicial, caso estejam presentes os requisitos do artigo 22 do Marco Civil da Internet, os quais devem ser comprovados pela parte requerente.

Uma vez não cumpridos os requisitos do art. 22, e deferido o pedido de fornecimento de dados, estar-se-á diante de uma violação ao princípio da privacidade e da proteção aos dados pessoais, garantidos pelos artigos 3º, II, III, 7º, I, II, III, VII, VIII, IX, X, 8º, 10, todos do Marco Civil da Internet, e pelo artigo 5º, X, da Constituição Federal.

Ocorre que, até 2022, esses direitos eram tidos como meros direitos garantidos aos usuários que utilizavam do serviço fornecido pelo provedor de aplicações de internet. No entanto, no ano de 2022, a Emenda Constitucional nº 115 foi promulgada e inseriu a proteção aos dados pessoais no rol de direitos fundamentais:

> "Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:
> "Art. 5º .....
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Segundo o artigo 5º, inciso I, da Lei Geral de Proteção de Dados, os dados pessoais são informações relacionadas à pessoa natural identificada ou identificável. Os dados armazenados por provedores de aplicações de internet - registros de acesso e número de IP -, são dados pessoais, na medida em que, como visto nos capítulos acima, eles são passíveis de identificar o usuário titular dos dados.

Assim, é evidente que os dados que os provedores de aplicações de internet estão obrigados a armazenar e fornecer em um processo judicial (registros de acesso e número de IP) são alcançados pelo direito fundamental de proteção aos dados pessoais inserido pela Emenda Constitucional nº 115/2022.

Como se sabe, os direitos fundamentais são intrínsecos aos seres humanos. Segundo Juliano Taveira, os direitos fundamentais são um "*conjunto de direitos estabelecidos por*

determinada comunidade política organizada, com o objetivo de satisfazer ideais ligados à dignidade da pessoa humana sobretudo a liberdade, a igualdade e a fraternidade"[42].

A necessidade da Emenda Constitucional nº 115/2022 surgiu justamente com o avanço da internet e com o comprometimento desses milhares de dados que são coletados pelos provedores de aplicações de internet. Inclusive, a justificativa da PEC nº 17/2019, que deu origem à Emenda, diz o seguinte:

> "A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão. O avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados. (...) De fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado".

Como o tratamento dos dados pessoais é uma atividade de risco que vem tomando cada vez mais espaço nas atividades, nada mais justo do que inserir a proteção aos dados pessoais no rol dos direitos fundamentais. Para Danilo Doneda:

> "Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados - que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental"[43].

Já para Rodrigo Pacheco, "o novo mandamento constitucional reforça a liberdade dos brasileiros, pois ele vem instalar-se em nossa Constituição em socorro da privacidade do cidadão. As informações pessoais, pertencem, de direito, ao indivíduo e a mais ninguém". Daí, portanto, a importância da Emenda Constitucional nº 115/2022, que garante ao indivíduo o direito fundamental de o seu dado ser apenas seu, e de mais ninguém.

Contudo, conforme visto anteriormente, esses dados, ainda que pertençam somente ao seu titular, podem ser armazenados e fornecidos em sede judicial. Para tanto, é necessário que os requisitos do artigo 22 do Marco Civil da Internet estejam preenchidos, especificamente a comprovação de fundados atos ilícitos cometidos pelo usuário.

---

[42] Direito Constitucional: Tomo I - Teoria da Constituição. p. 669.
[43] A proteção dos dados pessoais como um direito fundamental. p. 92.

Esse procedimento de fornecimento de dados em sede judicial já existia há muito tempo, antes de a Emenda Constitucional 115/2022 ser promulgada. A diferença, agora, é que, com a inserção da proteção aos direitos pessoais no rol de direitos fundamentais, caso os dados sejam fornecidos sem a observância da ocorrência de um ato ilícito, estar-se-á a violar um direito fundamental, e não mais apenas um direito meramente infraconstitucional.

Com a promulgação da Emenda, o artigo 22 do Marco Civil da Internet ganha um destaque e uma força maior, de modo que o juízo deverá ter uma cautela ainda maior ao analisar um pedido de fornecimento de dados em um processo judicial, sob pena de violar um direito fundamental do indivíduo.

Ora, se a proteção aos dados pessoais é garantia fundamental e tais dados pertencem só ao indivíduo, uma vez fornecidos esses dados em um procedimento judicial, o sigilo é quebrado. Isso porque, não é mais apenas o usuário e o provedor de aplicações de internet que possuem aqueles dados, mas sim o requerente, o advogado do requerente, o juízo, e qualquer outra pessoa que acesse o procedimento em questão.

O que se quer dizer é: uma vez fornecidos os dados no processo judicial, o sigilo estará quebrado. É evidente que isso pode ocorrer sem que haja uma violação ao sigilo, mas para que isso aconteça, a legislação deve ser observada e respeitada. Assim, a parte requerente deverá comprovar os fundados atos ilícitos, bem como o juízo deverá analisar, com cautela, se, de fato, o usuário cujo os dados se requer cometeu ato ilícito na rede social. Caso contrário, os dados não deverão ser fornecidos.

Relembrando os exemplos mencionados no capítulo anterior: caso o pedido de fornecimento de dados do administrador do grupo, que não cometeu nenhum ato ilícito contra o requerente ou contra qualquer outra pessoa, seja deferido, terá um direito fundamental violado. O mesmo ocorrerá com o usuário que curtiu a publicação, caso o fornecimento de seus dados seja deferido.

Ao longo de toda a exposição feita, a importância e a relevância dos dados armazenados pelos provedores de aplicações de internet foram destacadas. Isso porque, é através desses dados que se identifica um usuário dentre milhões de outros que navegam diariamente na internet. Assim, o que se vê, é uma tendência a proteger cada vez mais tais dados, na medida em que foi criada a Lei Geral de Proteção de Dados, o Marco Civil da Internet e, agora, a Emenda Constitucional nº 115/2022.

Como esses dados estão cada vez mais sendo tratados com cautela, não se pode a parte, em um processo judicial, nem o Juízo, ao analisar o feito, tratar os dados como se nada

fossem. Daí a importância de sempre seguir o procedimento previsto legalmente, sob pena de se violar direitos fundamentais dos indivíduos.

Em suma, a Emenda Constitucional nº 115/2022 veio para fortalecer ainda mais os princípios da privacidade e da proteção aos dados pessoais garantidos constitucionalmente e infraconstitucionalmente. Dessa forma, os impactos de tal Emenda nos procedimentos judiciais onde se requer ao provedor de aplicações de internet dados de um usuário para identificá-lo são claros: o cuidado e a atenção ao se requerer os dados, ou ao analisar o caso, deverá ser redobrado. Caso contrário, o usuário terá o seu direito fundamental de proteção aos seus dados pessoais violados.

5. CONCLUSÃO

De início, verifica-se que, ao longo do tempo e com o avanço da internet, os dados pessoais e a proteção dos mesmos foi ganhando importância legislativa e jurisprudencial. Com a utilização das redes sociais em massa, os provedores de aplicações de internet, que são os responsáveis por propiciar aos usuários o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet - ou seja, as redes sociais -, foram armazenando dados de milhares de usuários, que são difíceis de serem tratados e exigem cuidado especial, por serem extremamente pessoais e caracterizarem a individualidade de cada usuário.

Assim, os provedores coletam e armazenam milhares de dados de pessoas do mundo inteiro, e é claro que tais dados devem estar em um ambiente seguro, para que não sejam compartilhados com terceiros de forma ilícita. É nesse momento, inclusive, que o direito à privacidade e à proteção dos dados pessoais - que estão garantidos no Marco Civil da Internet - se destacam, na medida em que, ao compartilhar os dados com o provedor, os mesmos devem ser tratados na forma da lei, de forma segura.

É por isso que o Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, em seu artigo 13, dispõe sobre as diretrizes de padrões de segurança que devem ser observados pelos provedores de conexão e aplicações ao armazenar e tratar os dados pessoais coletados e as comunicações privadas.

A título de exemplo, tal Decreto dispõe que o acesso aos dados deve ser restrito e exclusivo para determinadas pessoas, bem como determina que os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, sendo que tais dados devem ser excluídos assim que cumpridas as hipóteses legais. Tudo isso para garantir a segurança dos dados obtidos dos usuários, bem como o direito à privacidade.

A partir disso, o Marco Civil da Internet, que é a legislação responsável por normatizar as relações entre o provedor de aplicações de internet e o usuário, estabelece, em seu artigo 15 da Lei, que os provedores de aplicações de internet estão obrigados a armazenar e fornecer somente os registros de acesso do usuário, o que inclui o número de IP e a data e hora de acesso, pelo prazo de 6 meses. Nesse sentido, os únicos dados que os provedores estão obrigados a fornecer nos processos judiciais em que se busca a identificação de um usuário, são os registros de acesso - os quais já foram reconhecidos como suficientes para a identificação do usuário pela jurisprudência pátria.

Além disso, para que tais dados sejam fornecidos no processos judicial, é necessário que se tenha uma ordem judicial com tal determinação, bem como que o requerente, ao formular o pedido, cumpra com os requisitos do artigo 22, parágrafo único, do Marco Civil da Internet, dentre os quais está a comprovação de ilícitos pelo usuário. Caso contrário, o pedido não deverá ser deferido, sob pena de violação à privacidade e à proteção de dados pessoais previstas nos artigos 3º, II, III, 7º, I, II, III, VII, VIII, IX, X, 8º, 10, todos do Marco Civil da Internet.

No entanto, através da presente pesquisa, foi possível averiguar que, após a promulgação da Emenda Constitucional nº 115/2022, a proteção aos dados pessoais passou a ser garantia fundamental do indivíduo.

Dessa forma, os impactos da norma aos casos em que se requer ao provedor de aplicações de internet os dados de determinado usuário consistem em se ter maior cautela e atenção no momento de realizar o requerimento, bem como no momento de avaliar e deferir o requerimento, na medida em que, se o pedido for deferido sem a devida observância do fundado ato ilícito, previsto no artigo 22, parágrafo único, do Marco Civil da Internet, o usuário não terá mais apenas um direito infraconstitucional violado, mas sim um direito fundamental violado.

REFERÊNCIAS

ALEXY, Robert. Teoria dos direitos fundamentais. Tradução de Virgílio Afonso da Silva. São Paulo, Editora Malheiros, 2008.

BERNARDES, Juliano Taveira; VIANNA, Olavo Augusto; FERREIRA, Alves. Direito Constitucional: Tomo I - Teoria da Constituição. 10ª edição. Salvador: JusPODIVM, 2020.

BIONI, Bruno Ricardo. Proteção de dados pessoais a função e os limites do consentimento. 3. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo. Proteção de dados pessoais. São Paulo: Forense, 2018.

BITTAR, Carlos Alberto. Os direitos da personalidade. 8. ed. São Paulo: Saraiva, 2014.

BRASIL. Senado Federal. Proposta da Emenda à Constituição nº 17/2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inlinebr. Acesso em 25 de maio de 2023.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. Scielo Brasil, 2017. Disponível em: <https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?lang=pt. Acesso em 03 de março de 2023.

DONEDA, Danilo. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law, v. 12, n. 2, p. 91/108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 25 de maio de 2023.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª edição. São Paulo, Editora Revista dos Tribunais, 8 de novembro de 2019.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. Revista de Direito Brasileira, [S.l.], v. 23, n. 9, p. 284-301, fev. 2020. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343>. Acesso de 25 de maio de 2023.

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, 2008.

GONÇALVES, Victor Hugo Pereira. Marco Civil da Internet comentado. 1. ed. São Paulo: Atlas, 2017.

GONÇALVES, Ana Catarina Piffer; MARTIN, Andréia Garcia. Os direitos à intimidade e à privacidade sob a perspectiva processual: a tutela inibitória dos direitos de personalidade, 2012.

JESUS, Damásio de; MILAGRE, José Antonio. Marco Civil da Internet: comentários à lei n. 12.965, de 23 de abril de 2014. 1ª edição. São Paulo: Saraiva, 2014.

LEITE, George Salomão; LEMOS, Ronaldo. Marco Civil da Internet. São Paulo: Atlas, 2014.

MACIEL, Rafael Fernandes. A requisição judicial de registros de conexão e aplicações no Marco Civil. *In: Direito & Internet III: Marco Civil da Internet*. Tomo II. DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). São Paulo: Quartier Latin, 2015.

MALDONADO, Viviane Nobrega Maldonado e BLUM, Renato Opice (coordenadores). LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019.

MARINELI, Marcelo Romão. Privacidade e Redes Sociais Virtuais: Sob a égide da Lei nº 12.965/2014 - Marco civil da internet. 1ª edição. Rio de Janeiro: Lumen Juris, 2017.

MENDES, Laura Schertel. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental, 1ª edição. São Paulo: Editora Saraiva, 27 de fevereiro de 2014.

OLIVEIRA, Carlos Murilo Rossi Trettel. Comportamento decisório no contexto big-data - um estudo de caso em uma companhia de GLP da região sudeste do Brasil. Medianeira, 2019.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) – 2. ed. – São Paulo: Saraiva Educação, 2020.

PINHEIRO, Patricia Peck. Direito digital. 6ª ed. rev. São Paulo: Saraiva, 2016.

ROBL FILHO, Ilton Norberto. Direito, intimidade e vida privada: paradoxos jurídicos e sociais na sociedade pós-moralista e hipermoderna. Curitiba: Juruá, 2010.

SARLET, Ingo Wolfgang. Eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11ª edição. Porto Alegre: Livraria do Advogado Editora, 2012.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. 11 de março de 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental>. Acesso em 15 de maio de 2023.

SILVA, José Afonso. Aplicabilidade das normas constitucionais. São Paulo: Malheiros, 2015.

SILVA, Sivaldo Pereira. Comunicação Digital, economia de dados e racionalização do tempo: algoritmos, mercado e controle de era dos bits. Contracampo, Niterói, v. 38, n. 01, p. 157-169, abr. 2019/jul. 2019.

SILVA, Virgílio Afonso da. Direitos Fundamentais conteúdo essencial, restrições e eficácia. 2. ed, 3ª tiragem. São Paulo: Malheiros, 2014.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; Bottino, Celina. Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017.

TEIXEIRA, Tarcisio. Direito digital e Processo eletrônico. 5ed. São Paulo Saraiva, 2020.

TEIXEIRA, Tarcisio. Marco Civil da Internet: comentado. São Paulo: Almedina, 2016.

TIBÚRCIO, Ana Luiza. Emenda Constitucional 115/2022: direito à proteção de dados pessoais. 2022. Disponível em: https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/. Acesso em 30 de maio de 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação, 2007.

WIMMER, Miriam. Proteção de dados pessoais em uma economia movida a dados. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Disponível em: https://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=349408&as. Acesso em 30 de maio de 2023.