A POSSIBILIDADE DE CONSERVAÇÃO DO REGISTRO DE CONEXÃO À LUZ DA JURISPRUDÊNCIA EUROPEIA E A SUA CONTRIBUIÇÃO PARA O CENÁRIO BRASILEIRO

THE POSSIBILITY OF PRESERVATION OF CONNECTION RECORDS IN LIGHT OF EUROPEAN JURISPRUDENCE AND ITS CONTRIBUTION TO THE BRAZILIAN CONTEXT

Cinthia Obladen de Almendra Freitas[1]

Rui Miguel Silva[2]

Devilson da Rocha Sousa[3]

Heloísa Daniela Nora[4]

Resumo: A possibilidade de manutenção dos registros de conexão dos usuários da Internet, antes de representar uma ofensa ao direito de liberdade e privacidade, pode se apresentar como medida indispensável para a garantia de maior segurança no ambiente digital, bem como para a prevenção e o combate aos crimes cibernéticos. Por conta dessa importância, tanto a União Europeia como o Brasil se dedicaram a legislar sobre tais questões de modo a estabelecer regras e diretrizes para a abordagem e enfrentamento do tema. Contudo, tanto em território europeu quanto em solo brasileiro, tais normativas têm sido objeto de críticas e questionamentos ante as possíveis violações a direitos fundamentais que podem resultar. Busca-se identificar, a partir de análise jurisprudencial, se e em que medida a documentação e a manutenção do registro de conexão podem ser feitas e quais os ensinamentos que a experiência europeia pode oferecer ao Brasil. Para tanto, será feito uso do método de pesquisa indutivo e do procedimento de levantamento de dados. Como resultado, restou evidenciado que a posição do Tribunal de Justiça da União Europeia pode representar um bom direcionamento a guiar o judiciário brasileiro no que se refere à compatibilização do respeito aos direitos fundamentais e à garantia de maior segurança no ambiente digital.

1 Doutora em Informática pela Pontifícia Universidade Católica do Paraná (PUCPR); Professora da Escola de Direito da PUCPR; Professora Permanente e Coordenadora do Programa de Pós-Graduação em Direito (PPGD) da PUCPR; Membro da Diretora do Instituto Nacional de Proteção de Dados (INPD); Membro Consultor da Comissão de Direito Digital e Proteção de Dados da OAB/ PR; e-mail: cinthia.freitas@pucpr.br;

2 Doutor em Engenharia Electrotécnica e de Computadores pelo Instituto Superior Técnico (IST) da Universidade Técnica de Lisboa – Portugal; Professor do Instituto Politécnico de Beja (IPBeja) – Portugal; e-mail: rui.silva@ipbeja.pt;

3 Doutorando pelo Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná (PUCPR); Mestre em Direito Constitucional Contemporâneo pela Universidade de Santa Cruz do Sul (UNISC); Mestre em Direito pela Universidade do Minho (UMINHO) – Portugal; Especialista em Direito Constitucional e Direito Público; Advogado; Bolsista CAPES-PROCAD/ SPCF; e-mail: devilsonsousa@hotmail.com;

4 Advogada. Bacharel em Direito pela Pontifícia Universidade Católica do Paraná (2017-2021). Mestranda em direito pela mesma instituição de formação - Bolsista CAPES.

Palavras-chaves: Cibersegurança; dados pessoais; direitos fundamentais; jurisprudência; proteção de dados.

Abstract: The possibility of maintaining users' Internet connection logs, rather than representing an offense against the right to freedom and privacy, can be seen as an essential measure to ensure greater security in the digital environment, as well as for the prevention and combat of cybercrimes. Due to this importance, both the European Union and Brazil have dedicated efforts to legislate on such issues in order to establish rules and guidelines for approaching and addressing the topic. However, both in European and Brazilian territories, such regulations have been subject to criticism and questioning regarding the potential violations of fundamental rights they may entail. The aim is to identify, through jurisprudential analysis, whether and to what extent the documentation and maintenance of connection logs can be implemented and what lessons the European experience can offer to Brazil. To this end, the inductive research method and data collection procedure will be used. As a result, it has been evidenced that the position of the Court of Justice of the European Union may serve as a good guideline to direct the Brazilian judiciary in reconciling respect for fundamental rights with the guarantee of greater security in the digital environment.

Keywords: Cybersecurity; personal data; fundamental rights; jurisprudence; data protection.

1 INTRODUÇÃO

A revolução digital induziu mudanças significativas nas dinâmicas de interação, comunicação e execução de atividades na sociedade contemporânea. Essas transformações permeiam tanto atividades cotidianas quanto domínios especializados, incluindo – mas não se limitando – o setor de Segurança Pública. Esta revolução digital caracteriza-se pela integração ubíqua das Tecnologias de Informação e Comunicação (TICs), resultando em um impacto profundo e multifacetado nos padrões sociais e na forma como os indivíduos trocam e têm acesso à informação. Em um mundo cada vez mais conectado, questões como a possibilidade de manter os registros de conexão dos usuários à Internet, visando não apenas possibilitar a repressão da criminalidade, seja no ambiente digital ou físico, mas também prevenir sua ocorrência, apresenta-se como uma questão primordial.

Nesse sentido, tanto a União Europeia quanto o Brasil têm se dedicado à normatização dessas questões sob premissas similares. De um lado, buscaram evidenciar as diferenças entre o acesso à rede mundial de computadores proporcionado por provedores de acesso à Internet e provedores de aplicação. De outro lado, estabeleceram as regras pelas quais a manutenção dos registros de conexão em ambos os cenários deve ocorrer.

Dada sua amplitude e os riscos aos quais tais ações podem expor os usuários da rede mundial de computadores, este trabalho se concentra na abordagem adotada por ambas as realidades jurídicas – União Europeia e Brasil – em relação aos registros realizados pelos provedores de acesso à Internet. É importante destacar que tanto a União Europeia quanto o Brasil reconhecem a necessidade de regular este domínio a partir de premissas que buscam estabelecer, de um lado, diretrizes que possibilitem a efetividade das políticas de segurança pública, e, de outro, a proteção aos direitos individuais. Contudo, apesar da existência de regulamentações sobre o tema e de justificativas plausíveis para a necessidade de reinterpretação dos direitos civis no meio ambiente digital, ainda surgem diversos questionamentos sobre como esse tema pode impactar negativamente no exercício e na garantia de certos direitos, tais como o direito à privacidade.

Assim, este artigo tem como objetivo geral realizar uma análise jurisprudencial focada especificamente nas abordagens adotadas pela União Europeia e pelo Brasil no que tange as condições e hipóteses para manutenção dos registros de conexão de usuários da rede mundial de computadores por provedores de acesso e o referido rastreamento. O estudo busca compreender de que maneira e em que extensão a União Europeia tem conseguido equilibrar as questões de segurança pública e privacidade, e como as experiências e os desafios enfrentados no contexto europeu podem oferecer ensinamentos valiosos para o cenário brasileiro.

Para alcançar este objetivo, primeiramente, realiza-se uma análise sobre como é feita a identificação do usuário na rede mundial de computadores, com foco também em aspectos tecnológicos. Em segundo lugar, é conduzida uma análise jurisprudencial de decisões do Tribunal de Justiça da União Europeia (TJUE) quanto à possibilidade de conservação de dados pessoais a partir do armazenamento dos registros de conexão, examinando decisões proferidas na União Europeia que destacam aspectos relevantes para a concretização do tema. E, finalmente, insere-se o contexto brasileiro, buscando formas de aplicação e adequação das normativas já existentes.

O estudo não apenas destaca a importância em conciliar demandas de segurança no ambiente digital com a proteção de direitos individuais, mas também proporciona uma base sólida para uma discussão sobre práticas e regulamentações em vigor, contribuindo para a construção de políticas que atendam às necessidades de uma sociedade conectada. O artigo é resultado de projeto de pesquisa financiado

pelo Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/SPCF) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

2 A POSSIBILIDADE DE IDENTIFICAÇÃO DOS USUÁRIOS DA REDE MUNDIAL DE COMPUTADORES E SEUS ASPECTOS TÉCNOLÓGICOS E NORMATIVOS

Para repressão e combate aos crimes cibernéticos, a possibilidade de identificação dos usuários da rede mundial de computadores e o acesso ou rastreamento das conexões feitas em rede têm se apresentado como medidas cruciais tanto no que se refere à identificação de autoria e materialização do ilícito, quanto na responsabilização dos agentes.

Antes de se debruçar sobre como essa identificação pode ocorrer, é fundamental compreender as diferenças entre provedores de acesso à Internet e provedores de aplicação, visto que cada um desempenha um papel único na esfera das TICs. Provedores de acesso à Internet, também conhecidos como *Internet Service Providers* (ISPs), são entidades que proporcionam o acesso dos usuários à Internet, fornecendo a infraestrutura necessária para a conexão *online*. Eles desempenham um papel crucial na garantia da conectividade, oferecendo serviços como banda larga, DSL (*Digital Subscriber Line*), e conexões de fibra óptica (Meinberg Ceroy, 2015).

Em paralelo, os provedores de aplicação, muitas vezes referidos como *Application Service Providers* (ASPs), operam em um nível diferente, fornecendo software e serviços que podem estar baseados em nuvem computacional, de modo que os usuários os acessam e utilizam por meio da Internet. Estes incluem uma variedade de aplicações, desde plataformas de e-mail e redes sociais até serviços de armazenamento em nuvem e aplicativos de escritório (Meinberg Ceroy, 2015).

É relevante destacar que, no Brasil, a lei nº 12.965 de 2014, conhecida como Marco Civil da Internet, estabelece fundamentos importantes para o entendimento da infraestrutura digital. De acordo com o inciso V do artigo 4º desta Lei, a conexão à Internet é definida como "a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP" (Brasil, 2014). Além disso, o inciso VII caracteriza as aplicações de Internet como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (Brasil, 2014). Essas definições fornecem a base

legal necessária para a conceituação dos provedores de acesso à Internet e dos provedores de aplicações.

Já no cenário europeu não há uma definição expressa quanto a estes termos (Tele2 Sverige Ab, 2016). Ficando a cargo dos diversos regulamentos e diretivas que abordam as questões relacionadas ao acesso à Internet e aos serviços digitais apontarem um conceito generalista para ambos os termos. Dentre estas legislações, se destacam o Regulamento Geral sobre a Proteção de Dados (GDPR), que não define diretamente conexão à Internet ou aplicações de Internet, mas influencia como os dados pessoais coletados por esses meios devem ser tratados (União Europeia, 2016), a Diretiva de Serviços de Mídia Audiovisual (AVMSD) que regula os serviços de mídia na UE, incluindo aqueles prestados via Internet (União Europeia, 2010) e o Código Europeu das Comunicações Eletrônicas, que consolida as regras da UE para o setor de telecomunicações, abordando o acesso e a comunicação via internet sob uma perspectiva mais ampla de infraestrutura de rede e serviços de comunicação eletrônica (União Europeia, 2018).

Considerando que os provedores de acesso constituem a espinha dorsal da conectividade na Internet, os registros de conexões realizados por esses provedores se apresentam, frequentemente, como ferramentas cruciais na prevenção e no combate à criminalidade. No que se refere a identificação do usuário, esta é possível principalmente a partir da identificação do equipamento utilizado no acesso à rede mundial de computadores. Quanto a este aspecto, importa esclarecer que computadores, notebooks, smartphones e todo dispositivo que tem acesso à rede mundial de computadores, e que operam a partir de determinados protocolos de transferência de dados para se comunicarem – tais como HTTP, SMTP, etc. –, possuem um número de reconhecimento conhecido como *Internet Protocol* (IP). Esse protocolo de identificação funciona como um endereço que possibilita a identificação do equipamento informático quando este está conectado à rede mundial de computadores, permitindo assim que a máquina tenha/apresente uma posição única e inequívoca dentro da web (Vechia, 2019).

Por definição, os endereços de IP são formados por 32 bits, sendo representados por quatro conjuntos de números de 8 bits, separados por pontos. Para organizar os endereços de IP no mundo, faixas de endereçamento são definidas seguindo um padrão hierárquico, sendo a *Internet Assigned Numbers Authority* (IANA) a autoridade máxima responsável por essa organização, juntamente com outras

entidades, tais como a RIPE NCC (Europa, Asia Central e Oriental), ARIN (América do Norte) e a CGI.br (Brasil), que fazem essa organização a nível regional ou local (Vechia, 2019).

A existência do IP é importante, pois ele funciona como principal ferramenta de identificação de um usuário na rede mundial de computadores, sendo destacado muitas vezes como a mais relevante informação presente no registro de conexão. Ocorre que muitas vezes a simples identificação do IP não é suficiente para indicar a autoria de determinado ilícito, daí a importância do registro de conexão.

O registro de conexão se apresenta como um conjunto de dados que documenta as atividades de comunicação entre dispositivos em uma rede. Vechia (2019) destaca que o registro de conexão é compreendido como um conjunto de informações que possibilitam indicar a data, a hora de início e término de uma conexão à Internet, sua duração, localização e o endereço IP utilizado pelo terminal para envio e recebimento de pacotes de dados e informações, tal qual estabelecido no Marco Civil da Internet no inciso VI do artigo 4º (Brasil, 2014).

Ele é dedicado à documentação das informações referentes às interações na rede estabelecidas pelos dispositivos, excluindo especificamente o armazenamento dos conteúdos visualizados, acessados ou transmitidos pelos usuários. A gestão desses registros implica na prática de conservar e arquivar os dados de conexão por um período previamente definido e a partir de um processo que envolve a organização sistemática e o armazenamento seguro desses registros, garantindo sua integridade, confiabilidade e disponibilidade para consultas apenas dentro das hipóteses previstas em lei.

Considerando a relevância dessas informações e impulsionados por eventos criminosos significativos, como os atentados terroristas de Madrid em 2004 e de Londres em 2005, que foram orquestrados através da Internet, além da necessidade de aprimorar os processos investigativos no ambiente digital, diversos sistemas jurídicos, incluindo os da União Europeia e do Brasil, empenharam-se no desenvolvimento de normas e procedimentos adequados para orientar a questão dos registros de conexão (Masseno, 2014).

Na prática, o acesso aos registros de conexão desempenha um papel frequentemente considerado como crucial nos processos investigativos, vez que oferece provas fundamentais que contribuem significativamente na (i) viabilização da identificação dos endereços IP associados a atividades criminosa; (ii) identificação e

determinação da autoria de delitos; (iii) possibilitação de acompanhamento geográfica de dispositivos envolvidos em ilícitos digitais; (iv) elaboração da cadeia temporal das ações suspeitas, o que fornece um arcabouço cronológico essencial para a compreensão e resolução de casos; (v) rastreamento e identificação de padrões de comportamento ilícito na Internet; (vi) estabelecimento de conexões digitais entre suspeitos e atividades criminosas; entre outras (Vechia, 2019).

A capacidade de vincular atividades digitais específicas a localizações físicas e momentos precisos não apenas facilita a identificação de suspeitos, mas também reforça a cadeia de evidências, contribuindo para uma melhor investigação e fortalecimento das provas.

Em virtude destas possibilidades, mas também dos riscos atrelados ao uso indiscriminado destes dados, é que aqueles sistemas jurídicos se dedicaram a criar regras que fossem aptas a guiar o acesso e o uso deste conjunto de informações. Na Europa, as questões relativas ao registro de conexões estavam dispostas principalmente na Diretiva 2006/24/CE, de 15 de março de 2006, do Parlamento e do Conselho Europeu. Esta normativa tinha como objetivo tratar exclusivamente da conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas e de provedores de acesso à Internet, fossem aquelas realizadas em redes públicas, fossem as das redes privadas.

Segundo o item “1” do artigo primeiro, seu objetivo seria, a nível da União, possibilitar a harmonização das legislações dos Estados-Membros no que se refere às obrigações dos fornecedores de serviços de comunicação eletrônica (Internet, Intranet, entre outras) no que se refere à “conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro” (União Europeia, 2006). Sua aplicação, ainda, compreenderia tanto os dados de tráfego e de localização relativos a indivíduos ou empresas, como aqueles dados conexos que servissem a identificação do assinante ou o utilizador do serviço.

Além disso, de acordo com o que estabeleciam os artigos 3º e 5º da Diretiva, os dados que os provedores de serviços de comunicações eletrônicas deveriam reter incluiriam informações cruciais para identificar a origem e o destino de uma comunicação, determinar data, horário, duração e seu tipo, os equipamentos utilizados pelos usuários, além de possibilitar a localização da ferramenta de

comunicação móvel; para tal fim, dentro do processo de retenção, seria necessária a inclusão de dados como o nome e o endereço do assinante ou do utilizador registrado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços Internet (União Europeia, 2006).

Afora a Diretiva 2006/24/CE, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002 – também conhecida como "Diretiva e-Privacy", que tem como objetivo abordar o tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, autorizava[5] em seu artigo 15º, item "1", que os Estados Membros adotassem medidas legislativas que possibilitassem que dados de tráfego fossem conservados durante um período limitado nos casos em que essas restrições representassem um meio necessário, adequado e proporcional para salvaguarda da segurança nacional, da defesa, da segurança pública ou nos casos em que elas pudessem possibilitar "a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas" (União Europeia, 2002).

No Brasil, as questões relativas a essa temática são regulamentadas pela lei nº 12.965, de 23 de abril de 2014, mais conhecida como Marco Civil da Internet. Essa legislação, que define princípios, garantias, direitos e deveres para a utilização da Internet no país, e no inciso VI do artigo 5º, como destacado, traz uma definição técnica precisa sobre o que constitui um registro de conexão. Além disso, o artigo 13 da lei além de estabelecer o prazo de 12 (doze) meses como o mínimo para a conservação destes dados, também vem trazer as circunstâncias sob as quais essas informações podem ser acessadas, os critérios necessários para tal acesso, as condições aplicáveis e os agentes autorizados a realizar tal solicitação (Brasil, 2014).

Contudo, apesar da importância desse mecanismo para o combate aos cibercrimes e para a garantia de maior segurança no ambiente digital, as normativas que lhe dão operacionalidade foram e são alvo de questionamentos em seus respectivos sistemas jurídicos. Na Europa, o Tribunal de Justiça da União Europeia (TJUE) enfrentou estes questionamentos em duas oportunidades: em 2014, quando do julgado do caso *Digital Rights Ireland* – Acórdão de 08/04/2014 — Processos

[5] Como se verá mais adiante, em virtude dos efeitos do julgado Tele2 Sverige, a União Europeia trabalhou na atualização da legislação acerca da proteção de dados e de privacidade, o que resultou no Regulamento Geral de Proteção de Dados (RGPD), que entrou em vigor em 2018. O RGPD incorpora muitas das proteções de privacidade da Diretiva 2002/58/CE e-Privacy, incluindo as disposições relativas à retenção de dados de comunicação.

Apensos C-293/12 E C-594/12 *Digital Rights Ireland*, julgado este que culminou com a revogação da Diretiva 2006/24/CE, (MASSENO, 2018) e, em 2016, no caso *Tele2 Sverige* – Acórdão de 21/12/2016 — Processos Apensos C-203/15 E C-698/15 Tele2 Sverige e Watson, julgado este que, por sua vez, culminou na invalidação parcial da Diretiva 2002/58/CE (Silveira; Freitas, 2018).

Por trás de ambas as decisões proferidas pelo TJUE está a busca pela preservação e pela garantia do direito à privacidade e à proteção de dados pessoais, garantidos pela Carta dos Direitos Fundamentais da União Europeia (CDFUE), direitos estes que até podem sofrer determinadas restrições, desde que sejam garantidas salvaguardas adequadas aos cidadãos.

No Brasil, ainda que de forma adjacente[6], a legalidade desta medida está sendo objeto de discussão na Ação Direta de Inconstitucionalidade (ADI) 5.527, ajuizada em maio de 2016, que estava sob a relatoria da Ministra Rosa Weber e agora do Ministro Flávio Dino. Nesta ação, o Partido da República questiona a constitucionalidade dos artigos 10º e 12º, do Marco Civil da Internet. A ADI foi disponibilizada para julgamento em plenário virtual do Supremo Tribunal Federal (STF) na última semana do mês de setembro de 2023 (Brasil, 2023). Após o voto da ministra relatora da ação, o julgamento foi interrompido a pedido do ministro Alexandre de Moraes, que solicitou que a ação fosse discutida no plenário físico da Suprema Corte, desde então o tema não volto a ser pautado (Lopes, 2023).

Em seu voto, a Ministra Rosa Weber se limitou a abordar a questão da constitucionalidade da interrupção dos serviços de mensagens no Brasil, alegando que os bloqueios podem ser realizados “quando materialmente possível o seu cumprimento, nas hipóteses e na forma de lei que estabeleça prévio leque de infrações definidas como especialmente graves, a ponto de justificar a natureza da medida” (Brasil, 2023). Uma das hipóteses de interrupção ocorreria quando da não disponibilização ou falha na coleta e armazenamento dos dados de registro de conexão por parte dos provedores.

No voto, a Ministra não abordou as questões relativas às hipóteses e condições de guarda e disponibilização dos registros de conexão, apesar de tais

[6] O objeto principal da ação é "ver declarada a inconstitucionalidade da penalidade de suspensão temporária e de proibição de exercício das atividades, decorrente de descumprimento de ordem judicial por parte da empresa responsável por fornecer mecanismo de troca de mensagens via internet", entretanto, considerando que a integralidade do caput do artigo 10º faz parte do pedido de análise, cabe o enfretamento quanto as regras vigentes acerca do registro de conexão (Brasil, 2023).

temas terem sido destacados por entidades públicas envolvidas no julgamento. Esta omissão pode sugerir uma possível concordância com as normas estabelecidas pelo Marco Civil da Internet a respeito do tema (Brasil, 2023).

Considerando que assim como na União Europeia, a privacidade e a proteção dos dados pessoais são direitos fundamentais, já reconhecidos inclusive em outros julgados do Tribunal, o posicionamento já expressado pelo TJUE pode ser um farol importante a guiar a atuação do STF no enfrentamento dessa matéria, por esse motivo, a análise das duas principais decisões sobre o tema de registro de conexão proferidas pelo Tribunal Europeu se faz tão importante.

3 A JURISPRUDÊNCIA DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA QUANTO À POSSIBILIDADE E HIPÓTESES DE CONSERVAÇÃO DO REGISTRO DE CONEXÕES

Se por um lado a União Europeia não tem uma Constituição instituída, ao menos não no formato tradicional, sua Carta de Direito de Direitos Fundamentais (CDFUE) cumpre a função de elencar os Direitos e as Garantias Fundamentais reconhecidas aos cidadãos europeus (Silveira, 2011).

Dentre os direitos consagrados no bojo da CDFUE, no artigo 7º e 8º estão respectivamente os direitos a vida privada e respeito comunicações e o direito à proteção de dados pessoais (União Europeia, 2000), direitos este que, em suma, buscam garantir a proteção e a privacidade dos indivíduos em relação as suas comunicações e ao tratamento de seus dados pessoais, seja por parte de empresas ou pelo Estado (Silveira, 2011). Além de estabelecer um nível de proteção mais elevado a estes direitos, assim como aos demais direitos fundamentais, a Carta é clara ao destacar que o tratamento de dados no âmbito da União deve ocorrer de forma leal, dentro de limites específicos e estar amparado em um fundamento legítimo previsto por lei.

Cumpre destacar que, no seu artigo 52, a CDFUE (União Europeia, 2000) vem estabelecer ainda que os direitos previstos neste documento só poderão sofrer restrições de exercício quanto estas estiverem devidamente previstas por lei, e, o mais importante, desde que esta previsão respeite o conteúdo essencial daqueles direitos e liberdades (Silveira, 2011).

Quanto à abrangência e à interpretação dada à CDFUE, o TJUE tem ao longo dos anos adotado uma posição jurisprudencial extensiva e progressista,

reconhecendo inclusive a existência de efeito vinculativo deste documento perante as instituições da União Europeia e os Estados-Membros quando da aplicação do direito da União. Isso implica que autoridades e tribunais, tanto da União quanto dos Estados-Membros, devam necessariamente observar a CDFUE quando da tomada de suas decisões (Freixes, 2013).

Em virtude desse arcabouço protecionista e dessa realidade jurídica, na condição de guardião do direito da União, em duas oportunidades diferentes o Tribunal de Justiça europeu foi provocado a se manifestar acerca da legalidade e da proporcionalidade das diretivas que versavam sobre a extensão do conceito, condições de manutenção e guarda dos registros de conexões, bem como, das circunstâncias para acesso a estes conjuntos de dados. Considerando que as decisões proferidas em ambos os julgados são elucidativas para a compreensão do direito à privacidade dos dados em toda a sua extensão, assim como para a demarcação dos limites impostos pelos direitos fundamentais ao poder de polícia estatal, a interpretação destes julgados se apresenta como medida indispensável.

3.1 O DIGITAL RIGHTS IRELAND DE 2014 E O RESTABELECIMENTO DA AUTORIDADE DOS DIREITOS FUNDAMENTAIS

Em 2014, o TJUE se dedicou a analisar a conformidade e a extensão da Diretiva 2006/24/CE que, como já destacado, tinha como objetivo harmonizar, no espaço comum da União, as disposições relativas à obrigação de provedores de serviços de comunicações eletrônicas, como empresas de telefonia e provedores de acesso à Internet, de reter determinados dados de tráfego e localização gerados por seus usuários, por um período que poderia variar de seis meses a dois anos. Seu objetivo era possibilitar que as autoridades de segurança e de investigação pudessem de forma mais eficiente prevenir e investigar crimes cometidos no ou a partir do ambiente digital, em especial terrorismo, tráfico de drogas, pedofilia e outros crimes que tivessem a Internet como base de divulgação/ação.

A apreciação da Diretiva pela Corte se deu em decorrência de um reenvio prejudicial apresentado pela H*igh Court of Ireland* [7], que coloca em lados opostos a

[7] O julgado Digital Rights Ireland Ltd. do Tribunal de Justiça da União Europeia é resultado do apensamento de dois processos, o C-293/12, remetido ao Tribunal pela High Court (Irlanda) e resumido acima, e o processo C-594/12, remetido pela Verfassungsgerichtshof (Corte Constitucional) da Áustria. O processo austríaco também buscava o posicionamento do tribunal acerca da compatibilidade da lei

Digital Rights Ireland Ltd. (DRI), uma organização sem fins lucrativos fundada em 2005 com o objetivo de promover e proteger os direitos digitais dos cidadãos na Irlanda e na União Europeia, e o Estado Irlandês. O processo originário, iniciado ainda em 2006, teve como objetivo contestar a legalidade das medidas legislativas e administrativas tomadas pelo governo irlandês com vista a transpor a Diretiva 2006/24/CE (Digital Rights Ireland LTD, 2014).

Ao submeter o caso para apreciação, a Corte irlandesa pontuou que não poderia dirimir as questões relativas ao direito nacional sem que não fosse posta em causa a própria validade da Diretiva 2006/24, e por isso decidiu suspender o processo e submeter ao Tribunal de Justiça algumas questões prejudiciais que se apresentam como fundamentais para a resolução da demanda, dentre as quais: a) se as restrições de direitos impostas pelo Estado irlandês resultantes das exigências dos artigos 3°, 4° e 6° da Diretiva 2006/24/CE seriam compatíveis com o Tratado da União Europeia (TUE), uma vez que fazia uso de medidas de certo modo desproporcionais, desnecessárias ou inadequadas para alcançar objetivos legítimos; b) se a Diretiva 2006/24/CE seria compatível com o direito fundamental ao respeito pela integridade e pela preservação das comunicações, assim como o direito à vida privada, destacado no artigo 7º da CDFUE e com o artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH); e c) se a Diretiva 2006/24/CE seria compatível com o direito à proteção dos dados pessoais consagrado no artigo 8º da Carta (Digital Rights Ireland LTD, 2014).

Já no âmbito do processo C-594/12, remetido pela *Verfassungsgerichtshof* , a corte constitucional austríaca, e que estava apensado ao caso irlandês, integrando assim o mesmo julgado (Digital Rights Ireland LTD, 2014), o Tribunal foi provocada a se posicionar, dentre outras coisas, quanto aos seguintes aspectos: a) se os artigos 3° a 9° da Diretiva 2006/24 seriam compatíveis com os artigos 7°, 8.° e 11.° da CDFUE; e b) considerando que os artigos 52 e 54 da CDFUE resultam no princípio da salvaguarda de um nível de proteção mais elevado aos Direitos Fundamentais, quais os limites para as restrições que poderiam ser colocadas a estes direitos e se a

---

que transpôs a Diretiva 2006/24 para o direito interno austríaco (Bundes-Verfassungsgesetz). Entre os processos, havia argumentações um pouco distintas que, contudo, tinham o mesmo pano de fundo e convergiam no que se refere à proteção dos direitos fundamentais dos cidadãos europeus e a razoabilidade de medidas que buscassem limitar estes direitos.

Diretiva em questão possibilitava o uso de métodos razoavelmente adequados para o atingimento dos objetivos que se propunha (investigação policial).

É importante observar, como destaca Masseno (2014, p. 11), que antes desse julgado diversas Cortes e Tribunais nacionais, tais como os Tribunais Constitucionais da Romênia, da Alemanha e da República Checa, já tinham se deparado com o enfrentamento da matéria em termos semelhantes, quais sejam, a validade das leis que buscavam a transposição da Diretiva em questão e suas compatibilidades com os direitos fundamentais, em especial o direito à privacidade, a proteção dos dados e a integridade das comunicações, consagrados na CDFUE e nas Constituições nacionais, contudo, tendo em vista o princípio do Primado do Direito da União sobre os Direitos nacionais, os Tribunais dos Estados-Membros tinham atuação limitada no sentido de avaliar apenas se as leis em questão conflitavam com os direitos fundamentais consagrados no seu ordenamento jurídico.

A seu turno e antes de se adentrar especificamente ao mérito da decisão do Tribunal, é importante notar que esta Diretiva surge em um contexto e em um cenário singular na Europa, isso porque no período que antecede a sua criação, entre os anos de 2004 e 2005, os países europeus se encontravam pressionados e sujeitados pela crescente ameaça terrorista, situação esta que acabou por ocasionar uma visão e um posicionamento mais elástico acerca da possibilidade de restrições aos direitos fundamentais de privacidade e proteção de dados pessoais.

Quanto a este aspecto, cumpre destacar que a escolha legislativa feita pela União não pode nem de longe ser vista como um processo de ponderação entre direitos fundamentais, nos termos teorizados por Alexy (2019), em que os atores legislativos da União, diante da colisão entre direitos fundamentais, o da segurança e os da privacidade, da proteção de dados e do completo sigilo das comunicações, realizaram um processo de sopesamento que culminou com a proeminência daquele primeiro direito frente aos outros. O que aconteceu neste caso foi que a União assumiu a posição de enfrentamento do terrorismo e do crime organizado fazendo uso de ações que pudessem trazer maiores restrições a estes direitos fundamentais.

Esse posicionamento pode ser comprovado quando se observam os considerandos 8 e 11 da Diretiva (Comissão Europeia, 2006). No primeiro destes itens, resta destacado que o Conselho Europeu encarregou o Conselho da União

Europeia[8] a proceder, no âmbito da luta contra o terrorismo, com a análise de propostas que fossem aptas a possibilitar o estabelecimento de regras sobre a conservação de dados de tráfego das comunicações pelos provedores de acesso à Internet. Já no considerando 11, os órgãos se manifestaram claramente quanto ao fato de o Conselho Europeu, ante os ataques terroristas ocorridos em 13 de julho de 2005, ter defendido a tomada de decisões que possibilitassem aprovar medidas que possibilitasse o armazenamento dos dados de tráfego e dos dados de localização para a investigação, detecção e repressão de infracções penais (Comissão Europeia, 2006).

Assim é que, mais uma vez citando David Masseno (2018, p. 2), vê-se na diretiva de 2006 uma alternativa emergencial, com claras restrições hermenêuticas, como de fato acabou sendo reconhecido pelo acórdão do TJUE, que apesar de ter seguido todos os procedimentos e as diretrizes estabelecida nos tratados europeus e ter sido apoiada e amplamente defendida pelas instituições europeias e por considerável parcela da opinião pública, acabou gerando uma limitação e uma intervenção desproporcional na vida privada, em especial no que se refere a comunicação e proteção dos dados, dos cidadãos europeus.

É importante notar que as incoerências, as limitações e a desproporcionalidade da Diretiva foram apontadas desde logo pelo Advogado Geral Pedro Cruz Villalón quando da emissão do seu parecer (Digital Rights Ireland LTD, 2014). Segundo suas conclusões, a Diretiva de Retenção de Dados era contrária aos direitos fundamentais à privacidade e à proteção de dados pessoais consagrados na Carta dos Direitos Fundamentais da União Europeia. Ele apontou que a obrigação de reter os dados de registro das comunicações eletrônicas violava os princípios da

[8] Considerando as particularidades da estrutura administrativa europeia e a semelhança entre os nomes dos órgãos, se faz necessário esclarecer que, como se pode supor, que o Conselho Europeu e o Conselho da União Europeia são órgãos distintos e com funções diferentes. O Conselho Europeu é composto pelos chefes de estado ou de governo dos países-membros da UE, além do presidente da Comissão Europeia e tem como função definir as diretrizes políticas gerais da UE, orientando a ação da União em questões estratégicas e de grande relevância para a integração, como as políticas de segurança, a gestão da crise econômica e a definição das prioridades orçamentárias. Já o Conselho da União Europeia é o órgão legislativo e executivo que representa os interesses dos Estados-membros em diversas áreas de política da UE, como em temas que envolvem a política externa, a justiça, a economia e a agricultura, entre outras. O Conselho é composto por ministros dos governos dos países-membros, que se reúnem em diferentes formações, de acordo com a temática a ser tratada. Cada país tem um representante com direito a voto e o Conselho adota decisões vinculantes por maioria qualificada.

necessidade e da proporcionalidade, e que a diretiva não estabelecia garantias suficientes para proteger a privacidade dos cidadãos.

Por sua vez, o Tribunal, ao buscar responder às questões prejudiciais trazidas por ambos os processos (C-293/12 e C-594/12), primeiramente pontuou que, em relação à adequação e à conformidade da Diretiva 2006/24 com os artigos 7°, 8° e 11° da CDFUE, a extensão dos dados armazenados pelos provedores de acesso à Internet era tamanha que, além de possibilitar a identificação dos usuários, também acabava viabilizando estabelecer conexões precisas acerca da vida privada e das comunicações dos indivíduos cujos dados haviam sido conservados, tais como, alguns de seus hábitos, os lugares que frequentavam, a frequência da comunicação em rede, entre outros aspectos (Digital Rights Ireland LTD, 2014). Algo que, no entendimento do Tribunal, afrontava diretamente os direitos previstos naqueles artigos.

Ainda segundo o Tribunal, ao impor a conservação destes dados e permitir o acesso das autoridades nacionais competentes a eles, a diretiva acabava por derrogar, como destacou o advogado-geral nas suas conclusões, o regime de proteção do direito ao respeito da vida privada instituído pelas Diretivas 95/46 e 2002/58, em relação ao tratamento de dados pessoais no setor das comunicações eletrônicas, o que gerava uma ingerência despropositada ao direito fundamental à privacidade e a proteção dos dados pessoais (Digital Rights Ireland LTD, 2014).

Em relação a este último aspecto, da ingerência proporcionada pela Diretiva, o Tribunal foi claro ao destacar que, independentemente de as informações relacionadas à vida privada serem ou não sensíveis ou tendo os envolvidos sofrido ou não algum incômodo ou transgressão em decorrência do tratamento destes dados, a simples existência ou possibilidade do tratamento nestes termos já era suficiente para demonstrar a existência de uma intervenção indevida na vida privada, o que constituía uma interferência grave nos direitos fundamentais à privacidade e à proteção de dados pessoais, interferência esta não justificada pela necessidade de prevenção e combate à criminalidade.

Quanto à questão prejudicial acerca da adequabilidade da determinação de conservação dos dados para o atingimento dos objetivos prosseguidos pela Diretiva 2006/24 (União Europeia, 2006), o TJUE foi claro ao destacar que, mesmo considerando a crescente importância dos meios de comunicação eletrônica na vida em sociedade e, mais ainda, a importância dos dados presentes nos registro de

conexão como um instrumento útil nas investigações penais, em especial no que se refere ao combate e à prevenção a criminalidade em ambiente digital, com destaque ao crime organizado e ao terrorismo, fatores estes que *prima facie* poderiam demonstrar a adequação ao objetivo prosseguido pela dita Diretiva, ainda assim “tal objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para efeitos da referida luta” (Digital Rights Ireland LTD, 2014, p. 18).

Por fim, o Tribunal asseverou que, ao não estabelecer regras claras e precisas que fossem suficientes para delimitar a interferência nos direitos fundamentais consagrados nos artigos 7º e 8º da CDFUE (União Europeia, 2000), poder-se-ia deduzir que a Diretiva assumia uma posição significativamente intervencionista naqueles direitos fundamentais, o que poderia gerar grandes impactos à ordem jurídica da União, sem que, contudo, tal ingerência pudesse ser satisfatória e seguramente controlada e administrada.

Em conclusão, e uma vez que a proteção de dados de pessoais e o sigilo das comunicações, sigilo este que abarca também a ideia de monitoramento destas comunicações, é um direito fundamental protegido pelo ordenamento jurídico da União Europeia, qualquer medida adotada pela União ou pelos Estados-Membros que afetem ou limitem esses direitos devem ser estritamente necessárias e proporcionais aos objetivos legítimos perseguidos, por este motivo, os Estados-Membros não poderiam obrigar os provedores de acesso à rede reterem dados de comunicações de forma indiscriminada e generalizada, mas apenas em casos específicos e limitados, e somente se isso fosse estritamente necessário para atingir um objetivo legítimo e desde que houvesse garantias adequadas para proteger os direitos fundamentais das pessoas afetadas.

Quanto a este último aspecto, considerando a existência de outros meios técnicos aptos a possibilitar a prevenção e o combate aos crimes cibernéticos, tais como o rastreamento e a identificação do usuário e/ou do equipamento através do IP, a análise de redes, a análise de arquivos de log, o rastreamento de atividades ou conteúdos maliciosos, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, entre outras possibilidades técnicas (Eleutério; Machado, 2010), é difícil imaginar que qualquer medida que busque indiscriminadamente determinar a guarda e o arquivamento de um amplo conjunto de dados vinculados ao registro de conexão,

como no caso da Diretiva 2006/24/CE (União Europeia, 2006), atenda aos princípios da adequação, da razoabilidade, da necessidade e da proporcionalidade.

Por todos estes fatores, o Tribunal de Justiça acabou entendendo pela revogação integral da Diretiva 2006/24/CE (União Europeia, 2006), obrigando ainda Estados-Membros a adotarem legislações nacionais que cumprissem os requisitos do direito da União, em especial no que se refere a garantia de integridade das comunicações, privacidade e o acesso a dados pessoais dos usuários.

3.2 O JULGADO TELE2 SVERIGE DE 2016 E A AMPLIAÇÃO DAS GARANTIAS DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

Após o retorno do garantismo proporcionado em 2014 pelo julgado D*igital Rights Ireland*, novamente em 2016 o Tribunal de Justiça Europeu teve que se posicionar acerca da compatibilidade e da legalidade da retenção de dados de comunicações eletrônicas com os Direitos Fundamentais da União. Ao se debruçar sobre o julgamento “Tele2 Sverige”, o TJUE teve a oportunidade de ampliar e trazer outros aspectos e implicações quanto ao direito fundamental à proteção de dados pessoais (Tele2 Sverige AB, 2016).

O julgado em questão, resultante de um reenvio prejudicial feito pelo Tribunal Administrativo de Segunda Instância de Estocolmo[9], ainda no ano de 2015, opunha a *Tele2 Sverige AB*, uma empresa de telecomunicações que oferece serviços de telefonia móvel, telefonia fixa, banda larga e TV para clientes na Suécia e em outros países europeus, e o Estado sueco. No cerne da discussão estava a contrariedade da empresa à lei sueca de retenção de dados, lei esta que encontrava sua fundamentação e sustentação na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 (Tele2 Sverige AB, 2016).

A Diretiva 2002/58/CE é uma diretiva da União Europeia que trata da proteção da privacidade no setor das telecomunicações. Também conhecida como Diretiva sobre Privacidade e Comunicações Eletrônicas, a legislação estabelece as regras para coleta, uso e processamento de dados pessoais pelos prestadores de serviços

[9] Assim como no julgado Digital Rights Ireland, o julgado Tele2 Sverige foi composto por dois processos apensos, o C-203/15, que opunha as partes acima destacadas, e o C-698/15, que opunha Tom Watson, Peter Brice e Geoffrey Lewis ao Ministro da Administração Interna do Reino Unido da Grã-Bretanha e da Irlanda do Norte e que tinha como ponto de controvérsia a legalidade e a conformidade com o direito da União da section 1 do Data Retention and Investigatory Powers Act 2014, uma Lei de 2014 que tratava da conservação de dados e os poderes de investigação das autoridades policiais daqueles países.

de comunicações eletrônicas e de acesso à Internet. Ela busca harmonizar as disposições dos Estados-Membros de forma a garantir um nível adequado de proteção dos direitos e das liberdades fundamentais, em especial o direito à privacidade, quando do tratamento de dados pessoais pelo setor das comunicações eletrônicas (União Europeia, 2002).

A normativa exige que os provedores de acesso à Internet adotem medidas adequadas para proteger a privacidade de seus clientes, incluindo a proteção de dados pessoais, a confidencialidade das comunicações eletrônicas e a segurança das redes de telecomunicações. A Diretiva também estabelece a obrigatoriedade de notificação em caso de violações de dados e define as regras para instalação e uso de cookies e outras tecnologias de rastreamento em sites da web. Afora estes pontos, a Diretiva também fixa as diretrizes para o acesso aos dados de tráfego e localização pelos órgãos de segurança pública e autoridades governamentais.

Tem-se que o objetivo desta legislação é possibilitar a proteção e a privacidade dos indivíduos, limitando o acesso a informações sensíveis e garantindo que as autoridades só tenham acesso a esses dados em casos específicos e com as devidas garantias legais e processuais (União Europeia, 2002).

Ou seja, diferentemente da Diretiva 2006/24/CE (União Europeia, 2006), a Diretiva 2002/58/CE atua(va)[10] com vistas a proteger os cidadãos europeus de acessos e tratamentos indevidos a seus dados pessoais (Tele2 Sverige AB, 2016). É importante notar que, por ser anterior aos anos de apreensão e medo causado pelo terrorismo e pelo crime organizado, por detrás de seus objetivos não pairava nenhuma sanha repressora ou fiscalizadora comparável ao *Big Brother* de Orwell, como era o caso da Diretiva de 2006.

Apesar de todo este arcabouço protecionista e garantista, a Diretiva sobre Privacidade e Comunicações Eletrônicas trazia no seu artigo 15, item 1, como já destacado acima, a possibilidade de os Estados-Membros poderem adotar medidas legislativas que, em alguma medida, restringissem os direitos e as garantias estabelecidas por ela, sempre que essas ações constituíssem “uma medida necessária, adequada e proporcionada numa sociedade democrática para

[10] Considerando que, a partir do julgado Tele2 Sverige, de 2016, a União Europeia trabalhou na atualização da legislação de proteção de dados e da privacidade, o que culminou com o surgimento do Regulamento Geral de Proteção de Dados (RGPD), que entrou em vigor em 2018, pode-se apontar esta nova normativa como a principal disposição a nível da União que atua como garantia e proteção da privacidade e dos dados pessoais dos cidadãos europeus.

salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais" (União Europeia, 2002, p. 10).

Foi com base nesta possibilidade que o legislador sueco, tensionando a transposição da Diretiva para o direito pátrio Sueco, alterou a *Lagen (2003:389) om elektronisk kommunikation*, também conhecida como LEK ou EK-Lagen, e o *Förordningen (2003:396) om elektronisk kommunikation*, também conhecido como regulamento CE ou regulamento PUL – ambas responsáveis por abordar o tema da prestação de serviços de comunicação eletrônica e da proteção de dados pessoais e privacidade no território sueco, com vias a possibilitar a conservação do registro de conexão e o acesso a esses dados pelas autoridades nacionais suecas (Tele2 Sverige AB, 2016).

Foi por conta destas alterações e de suas extensões que a Tele2 Sverige (processo C-203/15) entrou com uma demanda contra a *Post-och telestyrelsen*, a autoridade sueca de supervisão dos correios e telecomunicações (Tele2 Sverige AB, 2016). A ação se deu pelo fato de a empresa entender que a obrigação de armazenar dados de tráfego e de localização dos seus clientes violava a privacidade destes, pondo em causa a própria segurança dos dados pessoais, situação esta que seria contrária aos direitos consagrados na Carta dos Direitos Fundamentais da União Europeia.

Aqui cabe destacar que, por razões semelhantes, Tom Watson, Peter Brice e Geoffrey Lewis ingressaram com ação contra o Ministro da Administração Interna do Reino Unido da Grã-Bretanha e da Irlanda do Norte (processo C-698/15) (Tele2 Sverige AB, 2016). No caso em questão, as partes autoras argumentavam que o *Section 1* do *Data Retention and Investigatory Powers Act 2014*, lei de 2014 sobre a conservação de dados e os poderes de investigação, também violava o direito fundamental à proteção de dados e a CDFUE, uma vez que possibilitava a retenção generalizada e indiscriminada de dados de comunicações eletrônicas (Tele2 Sverige AB, 2016).

Diante destas controvérsias e alegações, tal como no caso *Digital Rights Ireland*, o Tribunal de Justiça foi provocado a se posicionar e emitir um parecer, uma vez que se tratava de controvérsia que envolvia, de fato, questionamentos quanto à própria validade daquela parte da Diretiva (Tele2 Sverige AB, 2016). Assim, o Tribunal teve que se debruçar sobre as seguintes questões prejudiciais trazidas por aqueles

dois processos: a) a interpretação dos artigos 7°, 8° e 52º, n. 1, da CDFUE (União Europeia, 2000) a partir do que dispõe o artigo 15º, n.1, da Diretiva 2002/58 (União Europeia, 2002) e amparado na argumentação da luta contra a criminalidade, autorizando que os Estados-Membros criem regulamentações que possibilitem uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização de assinantes e utilizadores de serviços de comunicação eletrônica; b) o artigo 15º n. 1 interpretado a partir destes artigos da CDFUE (União Europeia, 2000), que pode ser entendido como opositor a uma regulamentação nacional que busque garantir proteção e a segurança dos dados de tráfego e dos dados de localização, em especial o acesso das autoridades nacionais competentes aos dados conservados, sem limitar esse acesso apenas para efeitos de luta contra a criminalidade em ambiente digital, sem submeter tal acesso a um controle prévio por um órgão jurisdicional ou por uma autoridade administrativa independente e sem exigir que os dados em causa sejam conservados no território da União.

Em suas conclusões sobre o caso, Henrik Saugmandsgaard, então advogado geral, pontuou que a possibilidade de acesso indiscriminado aos dados de tráfego e de localização de provedores de Acesso à Internet se caracteriza como uma interferência desproporcional nos direitos fundamentais à privacidade e proteção de dados pessoais. O advogado destacou ainda que tal prática não poderia ser justificada mesmo para fins de segurança nacional ou investigação criminal (Tele2 Sverige AB, 2016).

Ademais, ainda segundo seu parecer, se um Estado-Membro intentar impor uma obrigação geral de retenção de dados de tráfego e localização, além de essa medida ser válida apenas em casos excepcionais, faz-se necessário que tal obrigação seja acompanhada de medidas adequadas de proteção de dados e limitações claras de uso e acesso a esses dados, o que na situação em questão não existia (Tele2 Sverige AB, 2016).

Diante deste posicionamento, que apesar de não ser vinculante contribui significativamente para a interpretação e posição do Tribunal, e considerando a decisão já proferida no julgado anterior, não é de se estranhar que o TJUE tenha concluído que o artigo 15., n.o 1, da Diretiva 2002/58 (União Europeia, 2002), lido à luz dos artigos 7.°, 8.° , 11º e 52º, n.o 1, da CDFUE (União Europeia, 2000) deve ser entendido como em contraposição a uma regulamentação nacional que possibilite, para efeitos de luta contra a criminalidade, a manutenção generalizada e

indiferenciada do registro de conexão dos assinantes ou utilizadores de um determinado serviço de comunicação eletrônica.

Sem esgotar a questão, a Corte asseverou que este mesmo dispositivo deve ser interpretado como oposição a qualquer ação dos Estados-Membros que busque regular a proteção e a segurança dos dados de tráfego e dos dados de localização sem limitar o acesso ou a submissão deste, mesmo no âmbito da luta contra a criminalidade, “a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União” (Digital Rights Ireland Ltd, 2014, p. 26).

Esse posicionamento do tribunal acabou gerando três grandes consequências: a) houve o fim da retenção ampla de dados, uma vez que, a partir daquele momento, os provedores de serviços de acesso à Internet não poderiam mais reter indiscriminadamente o registro de conexão de seus clientes; b) serviu para reforçar a proteção à privacidade dos indivíduos, ficando claro que a retenção de dados de comunicações eletrônicas só poderia ser feita com base em razões específicas e limitadas, como a prevenção ou investigação de crimes graves; e c) limitou o acesso das autoridades aos dados pessoais, uma vez que, a partir daquele momento, estas só poderiam solicitar esses dados para fins específicos e limitados, e apenas quando não houvesse outras formas de obter as informações necessárias.

4 O CONTEXTO BRASILEIRO E OS POSSÍVEIS CAMINHOS A SEREM SEGUIDOS

Inicialmente, cumpre destacar que não há necessidade da realização de um estudo comparado aprofundado entre o sistema jurídico da União Europeia e a ordem jurídica brasileira para que os julgados acima analisados possam ser considerados como um norte para o judiciário brasileiro, e isso se dá por dois fatores principais. O primeiro deles se encontra no fato de que nos dois ordenamentos jurídicos o direito à privacidade, a proteção dos dados pessoais e ao sigilo das comunicações - sigilo aqui entendido também como o direito de o Estado não saber quando ou como alguém se comunica, foram elevados à condição de direito fundamental, ou seja, estes direitos encontram o mesmo grau de proteção em ambas as realidades.

O segundo fator se coaduna na semelhança e na conexão que existe entre a tradição constitucional do Direito brasileiro e a predominante no Direito Europeu, semelhanças estas que acarretam o enfrentamento e a compreensão da temática dos

direitos fundamentais sobre as mesmas perspectivas e com os mesmos graus de proteção (Tavares, 2013).

Afora estes fatos, como destacado no item 1 do presente trabalho, assim como no cenário da União Europeia, o Brasil também se preocupou em possibilitar e regular a conservação do registro de conexão, ação esta que se deu a partir do Marco Civil da Internet – lei 12.965, de 2014 (Brasil, 2014). No capítulo terceiro da Lei, entre os artigos 10º e 13º, o legislador brasileiro estabeleceu as regras referente a guarda, manutenção, segurança e acesso aos registros de conexão em termos semelhantes àqueles que foram estabelecidos nas Diretivas 2002/58/CE (União Europeia, 2002) e 2006/24/CE (União Europeia, 2006).

Ademais, ao dispor sobre este tema no Marco Civil da Internet, o legislador acabou reconhecendo, em termos semelhantes ao europeu, que o registro de conexão é uma importante ferramenta para a investigação e a repressão de crimes no ambiente digital, como terrorismo, fraudes, pornografia infantil, discurso de ódio, entre outros.

No mesmo sentido, e seguindo as mesmas premissas da União Europeia, preocupado com a proteção da privacidade dos usuários, a lei veio estabelecer que a manutenção do registro de conexão deve se dar em ambiente seguro e sigiloso, de forma a garantir a privacidade dos usuários e evitar o uso indevido das informações, devendo ainda o seu acesso sofrer algumas limitações e estar condicionado a determinadas premissas, dentre as quais, a necessidade de determinação judicial pela autoridade competente e seu uso estar limitado a investigações criminais ou para instrução de processos judiciais.

E neste ponto está a diferença mais marcante entre as duas realidades jurídicas. Enquanto o Marco Civil da Internet optou por primeiro conceituar o termo “registro de conexão” de forma clara e precisa - mais precisamente no inciso VI do artigo 5º (BRASIL, 2014), para depois se debruçar sobre o estabelecimento de suas regras, o conjunto normativo europeu falhou em claramente definir os limites deste conceito, em virtude desta ausência, a atuação dos provedores de Internet, dos Estados-Membros e dos órgãos de investigação no que diz respeito aos dados envolvidos nessas retenções se deu de forma mais extensa.

Apesar disso, uma leitura mais atenta da lei brasileira pode evidenciar a mesma falta de proporcionalidade, razoabilidade e adequação no uso do registro de comunicação como ferramenta de investigação e de produção de prova. Isso se dá

em especial por 03 (três) fatores: (i) o tempo mínimo que os dados devem ser armazenados; ii) a possibilidade de acesso destes dados por parte de órgãos administrativos; e (iii) a falta de fiscalização e controle no processo de coleta, manutenção e acesso a estes dados.

Quanto ao tempo de armazenamento, é relevante observar que a lei, especificamente em seu artigo 13º, obriga aos provedores de acesso à Internet a reter esses dados por um prazo mínimo de doze meses, prazo este que pode ser estendido a pedido da autoridade policial ou administrativa ou do Ministério Público. Levando em conta que os registros de conexão não são a única forma de se obter provas em investigações policiais a manutenção prolongada desses registros, conforme estabelecido pelo Marco Civil da Internet, levanta-se a questões sobre a adequação e proporcionalidade da medida.

Nesse sentido, cumpre destacar que a Lei Geral de Proteção de Dados Pessoais (LGPD) ao buscar garantir que qualquer tratamento de dados pessoais não apenas cumpra com requisitos legais previamente estabelecidos, mas também respeite os princípios de adequação (art. 6º, inciso II), necessidade (art. 6º, inciso III) e proporcionalidade (art. 6º, inciso III) vem reforçar esse argumento (Brasil, 2017). Assim, a prática de retenção extensiva de dados pode não só representar uma desproporcionalidade em termos de tempo e finalidade, como também oferecer um risco potencial à privacidade dos usuários, exigindo uma avaliação cuidadosa e crítica à luz dos direitos fundamentais à privacidade e à proteção de dados pessoais.

Acerca deste aspecto, Mendes e Doneda sustentam que a prática de manutenção prolongada de dados pessoais deve ser estritamente justificada por finalidades legítimas e específicas, em conformidade com os requisitos estabelecidos pela LGPD, sendo fundamental que tal retenção esteja amparada na necessidade e proporcionalidade com o objetivo perseguido (Mendes; Doneda, 2018, p. 472). Além disso, os autores enfatizam a necessidade de implementar salvaguardas robustas para proteger os dados durante o período em que são mantidos e de assegurar, ainda que em processos sigilosos, a transparência no tratamento desses dados (Mendes; Doneda, 2018). Da forma como ocorre atualmente, tais premissas não parecem ser atingidas.

No caso europeu, por exemplo, a retenção mínima exigida pela Diretiva 2006/24 era de seis meses, ou seja, metade deste tempo, podendo ser renovado por iguais períodos (União Europeia, 2006). Com o afastamento da Diretiva pelo TJUE,

além de ter havido o reconhecimento da necessidade de limitação do período de manutenção destes dados e das possibilidades de renovação, o Tribunal também sedimentou o entendimento de que, superado o tempo inicial de guarda, nunca superior a seis meses, a manutenção dos dados para fins de investigação deveria se limitar a alvos previamente estabelecidos e o pedido de conservação deveria ser embasado com o fundamento da necessidade e imprescindibilidade da medida (Tele2 Sverige AB, 2016).

Ademais, a retenção prolongada de dados aumenta significativamente o risco de violações de privacidade, não apenas no que se refere a possíveis ataques cibernéticos, mas especialmente em função de falhas de segurança. Nesse sentido, é importante ressaltar que sistemas de armazenamento de longo prazo podem se tornar obsoletos, tornando-os menos seguros contra as técnicas de invasão mais modernas e avançadas. Além disso, a gestão eficaz de grandes volumes de dados exige mecanismos de segurança atualizados e constantemente revisados, como criptografia de ponta a ponta, controle de acesso baseado em funções e monitoramento contínuo de atividades suspeitas. Sem essas salvaguardas, que não bem endereçadas no Decreto nº 8.771/2016, os dados armazenados não apenas ocupam espaço valioso de armazenamento, mas também permanecem vulneráveis a acessos não autorizados e uso indevido, contrariando princípios fundamentais da proteção de dados pessoais e da privacidade dos usuários.

Além disso, em cenários de exceção ou de uso indevido da estrutura estatal, essa prática poderia ser instrumentalizada para fins de perseguição e controle, colocando em risco as liberdades civis ao permitir um monitoramento ampla e indistinto da população.

Quanto ao segundo aspecto, que se refere à possibilidade de órgãos administrativos acessarem esses dados, o parágrafo segundo do artigo 13, ao estender a autorização para o acesso a essas informações não somente à polícia e ao Ministério Público, mas também a “autoridades administrativas”, amplia consideravelmente o espectro de agentes estatais habilitados a obter essas informações. Essa expansão no acesso é similar ao observado no contexto europeu, sendo que tal abrangência foi julgada como excessiva e desproporcional, em especial por não definir claramente que agentes administrativos seriam estes, sob quais hipóteses poderia haver estas solicitações e o como se daria o controle e salvaguarda destes dados pelos órgãos administrativos.

Acerca deste aspecto, Solove e Schwartz (2018), enfatizam que a falta de definições claras sobre quais agentes administrativos podem acessar dados pessoais e em que circunstâncias levanta sérias preocupações sobre a proteção da privacidade dos cidadãos. Além disso, como pontuado por Snowden (2019), o acesso não regulamentado e amplo a dados pessoais por múltiplas agências governamentais pode criar vulnerabilidades significativas, expondo os cidadãos a riscos de privacidade desproporcionais e potencialmente injustificados.

De outro lado, do ponto de vista técnico-informático, considerando que a complexidade e o volume substancial dos dados gerados em registros de conexão demandam uma infraestrutura avançada de armazenamento e processamento, bem como uma capacidade de gerenciamento eficientemente dessas informações, que incluem horários de acesso, duração das sessões, e IPs utilizados, (Hintzbergen et al, 2018), há sérias dúvidas sobre a capacidade dos órgãos administrativos em tratar seguramente estes dados

De outro lado, não se pode fechar os olhos ao desafio significativo relacionado à conformidade legal e a finalidade de uso destes dados por parte daqueles órgãos. Tal fato invariavelmente acarreta a necessidade de implementação de controles de acesso rigorosos e mecanismos de auditoria detalhados para garantir que somente pessoas autorizadas tenham acesso aos dados, que todas as operações sejam registradas e que estas obedeçam às finalidades especificadas previamente (Hintzbergen et al, 2018).

Mais uma vez, é importante destacar que permitir que uma gama tão vasta de atores públicos tenha acesso aos registros de conexão dos usuários pode levar a uma intrusão significativa na privacidade individual, ultrapassando os limites do que seria considerado necessário e proporcional à luz dos objetivos legítimos de investigação e da segurança pública. Esse acesso amplo e potencialmente irrestrito coloca em risco as garantias de privacidade, ao abrir precedentes para que esses dados sejam utilizados para além do escopo estritamente necessário para a condução de investigações, aumentando as preocupações com a vigilância estatal e o monitoramento da população sem salvaguardas adequadas.

Quanto à insuficiência na fiscalização e ao controle do processo de armazenamento e manutenção destes dados, é crucial notar que, apesar de a legislação estipular que os registros de conexão devem ser preservados sob sigilo, em um ambiente controlado e seguro, e que outras disposições legais relacionadas à

segurança e à neutralidade da rede também devem ser cumpridas, observa-se uma lacuna significativa no que tange à efetividade desse processo de fiscalização. Isso se dá pelo fato de o Decreto nº 8.771 de 11 de maio de 2016 (Brasil, 2016), que veio regular este tema, apesar de ter estabelecido os padrões de segurança para esta ação, não ter criado um processo de fiscalização e controle em si, tendo apenas definido que a Agência Nacional de Telecomunicações (ANATEL) e a Secretaria Nacional do Consumidor (SENACON) ficariam responsáveis por fiscalizar e eventualmente aplicar as sanções por descumprimento.

É importante destacar que essa lacuna, mesmo em um contexto em que os registros de conexão podem não revelar detalhes profundos sobre os usuários, os submete a uma série de vulnerabilidades, tais como vazamentos de informações, armazenamento e manutenção em desacordo às regras legais e cujos processos possuem pouca ou nenhuma transparência, controle ou fiscalização. Portanto, pode-se afirmar que a ausência de um controle eficaz por parte do governo sobre essas atividades críticas, embora não comprometa diretamente os objetivos dessa medida — o uso dos registros de conexão para o combate à criminalidade digital —, resulta em uma redução e relativização dos direitos dos cidadãos no ambiente digital de modo semelhante ao que ocorreu no caso europeu.

Desta forma, é essencial, no contexto brasileiro, assim como já observado na Europa, que o Judiciário examine, sob a égide dos direitos fundamentais à privacidade, a proteção de dados pessoais e de sigilo das comunicações, se as práticas e disposições estabelecidas pelo Marco Civil da Internet referentes à coleta e à retenção de registros de conexão estão em alinhamento com o princípio da proporcionalidade e constituem uma intervenção adequada na esfera dos direitos dos cidadãos no ambiente digital. Essa análise deve verificar se tais práticas ocorrem dentro dos limites legais definidos e se estão fundamentadas em bases legais legítimas, assegurando que o equilíbrio entre segurança, privacidade e liberdade dos cidadãos seja mantido.

Contudo, considerando que até o momento o tema do registro de conexão é tratado apenas de forma subjacente pela Supremo Tribunal, não havendo de fato nenhuma ação que busque questionar a constitucionalidade e a adequação da referida parte do diploma legal, a tendência é que tais questionamentos fiquem limitados à academia e não evoluam tanto no cenário jurisprudencial.

Ademais, mesmo a Ação Direta de Inconstitucionalidade 5.527 (Brasil, 2023), que foi proposta pelo Partido da República (PR) e que questiona diversos dispositivos da Lei nº 12.965/2014 (Brasil, 2014), não será suficiente para possibilitar o estabelecimento de um marco jurisprudencial sólido e estável quanto ao tema, uma vez que a corte direcionou seu foco exclusivamente para análise da adequação da suspensão dos serviços de comunicação eletrônica quando da não observância de decisões judiciais pelos fornecedores destes serviços.

Neste contexto, mesmo os julgados do Tribunal de Justiça da União Europeia podendo servir como importantes marcos referenciais quanto ao tema do registro de conexão e dos direitos fundamentais da privacidade e proteção de dados, o Brasil ainda ficará longe de estabelecer os mesmos *standards* de proteção aos seus cidadãos, não pelo fato de aqui aqueles direitos sofrerem menos limitações ou os titulares estarem menos expostos a violações, mas tão somente em virtude da falta de uma discussão e compreensão mais profunda sobre o tema.

5 CONCLUSÃO

O artigo explorou a importância e os desafios associados à conservação dos registros de conexão à Internet a partir de uma análise à luz da legislação e da jurisprudência europeia e da legislação brasileira. A análise revelou que, enquanto a Europa enfrentou significativos desafios legais e éticos relacionados à privacidade e à proteção de dados, culminando em decisões judiciais que estabeleceram limites e procedimentos referentes a retenção destes dados, o Brasil ainda não reservou a atenção necessária que o tema suscita.

Ficou evidenciado que a experiência europeia, a partir das decisões do Tribunal de Justiça da União Europeia, oferece importantes lições sobre o equilíbrio entre a necessidade de garantia da investigação e prevenção de crimes e a proteção à privacidade dos usuários da Internet. O estudo comprovou ainda que no Brasil, embora a legislação vigente ofereça um quadro para a conservação de dados, a implementação prática dessa medida em linha com os princípios de proporcionalidade e necessidade ainda representam desafios significativos.

Nesse sentido, a jurisprudência do Tribunal de Justiça da União Europeia sobre os limites e condições para a manutenção dos dados de registro de conexão dos usuários de serviços de provedores de acesso à Internet representa verdadeiro

marco protecionista no que se refere à garantia e à aplicação daqueles direitos em ambiente digital. Por este motivo e tendo em conta a semelhança entre ambas as realidades jurídicas, as decisões proferidas por aquele Tribunal podem servir como farol a guiar a atuação do Supremo Tribunal Federal, e do judiciário brasileiro, quando este tiver que enfrentar não apenas a legalidade e a adequação desta medida, mas também quanto estiver diante de questões que busquem analisar a extensão e validade das restrições aos direitos fundamentais neste ambiente.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Vigílio Afonso da Silva. São Paulo: Malheiros Editores, 2019.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar do tratamento de dados pessoais e da privacidade na internet. **Diário Oficial da União,** Brasília, DF, seção 1, 12 maio 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 07 maio 2024.

BRASIL. Lei **nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 maio 2024.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 maio 2024.

_____. Supremo Tribunal Federal. **A g .Reg. nos Emb .Decl**. Na medida cautelar e m mandado de segurança 38.169 distrito federal. Relatora: Min. Cármen lúcia. Jurisprudência do STF. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur462379/false. Acesso em: 07 maio 2024.

_____. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 5.527**. Relatora: Ministra Rosa Weber. Supremo Tribunal Federal. Julgamento iniciado em 27 de maio de 2023. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=560715474,. Acesso em: 07 maio 2024.

DAVID MASSENO, Manuel. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa, uma Cartografia das Fontes Legislativas. **Revista Eletrônica Direito & TI,** v.1, n.9, p.7, 2018. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/106. Acesso em: 07 maio 2024.

DIGITAL RIGHTS IRELAND LTD. V. Minister for communications and others. **ECLI:EU:C:2014:238**. 2014. 1 recurso online (42 p.). Relator: Vassilios Skouris.

Tribunal de Justiça da União Europeia, Luxemburgo, 8 de abril de 2014. Disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0293 . Acesso em: 07 maio 2024.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. **Desvendando a Computação Forense.** São Paulo: Novatec Editora, 2010.

FREIXES, Teresa. Carta de Direitos Fundamentais da União Europeia. *In*. SILVEIRA, Alessandra (coord.).; CANOTILHO, Mariana. **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra: Almeidina, 2013.

HINTZBERGEN, Jule; HINTZBERGEN, SMULDERS, André; Kess; BAARS, Hans. **Fundamentos de segurança da informação**: com base na ISSO 27001 e na ISSO 27002. Trad. Alan de Sá. Rio de Janeiro: Brasport, 2018.

LOPES, Leiliane. STF: Bloqueio de aplicativos de mensagens terá julgamento físico. **Pleno News,** 2023. Disponível em: https://pleno.news/brasil/stf-bloqueio-de-aplicativos-de-mensagens-tera-julgamento-fisico.html. Acesso em: 07 maio 2024.

MASSENO, Manuel David.. Que fazer, na UE, depois do Acórdão "Digital Rights Ireland'"? *In*: SIMPÓSIO DE SEGURANÇA INFORMÁTICA E CIBERCRIME, 5., 2014. **Anais** [...] Lab UbiNET / IPBeja, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 472, 2018.

MEINBERG CEROY, F. . Os Conceitos de Provedores no Marco Civil da Internet. **Revista Eletrônica Direito & TI**, [S. l.], v. 1, n. 1, p. 3, 2015. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/14. Acesso em: 07 maio 2024.

SILVEIRA, Alessandra. **Princípios de Direito da União Europeia**: Doutrina e Jurisprudência. 2. ed. Lisboa: Quid Juris Sociedade Editora, 2011.

SILVEIRA, Alessandra; FREITAS, Pedro Miguel. The Directive 2006/24 declaration of invalidity and the consequences of metadata retention in the EU Member States: A Fundamental Rights Standards Approach. **Law, State and Telecommunications Review,** [S. l.], v. 9, n. 1, p. 47–68, 2017. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21513. Acesso em: 07 maio 2024.

SNOWDEN, Edward. **Permanent Record**. São Paulo: Planeta do Brasil, 2019.

SOLOVE, Daniel J; SCHWARTZ, Paul M. **Information Privacy Law**. 6. ed. Nova Iorque: Editora Wolters Kluwer, 2018.

TAVARES, André Ramos; Comentários ao artigo 5º da Constituição Federal. *In*: CANOTILHO, J. J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva;Almedina, 2013.

TELE2 SVERIGE AB V. **Post-Och Telestyrelsen**. ECLI:EU:C:2016:970. 2016. 1 recurso online (19 p.). Relator: Koen Lenaerts. Tribunal de Justiça da União Europeia, Luxemburgo, 21 de dezembro de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62015CJ0203. Acesso em: 07 maio 2024.

UNIÃO EUROPEIA. **Carta de Direitos Fundamentais da União Europeia**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012P/TXT&from=PT. Acesso em: 07 maio 2024.

UNIÃO EUROPEIA. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva sobre privacidade e comunicações eletrônicas)**. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:HTML. Acesso em: 07 maio 2024.

_____. **Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas acessíveis ao público ou de redes públicas de comunicações**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32006L0024. Acesso em: 07 maio 2024.

VECCHIA, Evandro Dalla. **Perícia Digital:** da investigação à análise forense. 2. ed. Campinas: Millenium Editora, 2019.

_____. UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/EC (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia,** L 119, 4 de maio de 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 07 maio 2024.

_____. Diretiva 2010/13/EU do Parlamento Europeu e do Conselho de 10 de março de 2010 sobre a coordenação de certas disposições estabelecidas por lei, regulamento ou ação administrativa nos Estados Membros relativas à prestação de serviços de comunicação social audiovisual. **Jornal Oficial da União Europei**a, L 95, 15 de abril de 2010. Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0013. Acesso em: 07 maio 2024.

_____. Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho de 11 de dezembro de 2018 que estabelece o Código Europeu das Comunicações Eletrônicas (reformulação). **Jornal Oficial da União Europeia**, L 321, 17 de dezembro de 2018. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0160 . Acesso em: 07 maio 2024.