UNIVERSIDADE FEDERAL RURAL DO SEMIÁRIDO – UFERSA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS E HUMANAS – CCSAH
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS – DCSA
CURSO DE GRADUAÇÃO EM DIREITO

Lívia Andrade Albuquerque Valença

A PROTEÇÃO DO FLUXO INFORMACIONAL NA LEI DE INTERCEPTAÇÃO TELEFÔNICA E OS DESAFIOS DA PERSECUÇÃO PENAL

Mossoró/RN
2020

Lívia Andrade Albuquerque Valença

A PROTEÇÃO DO FLUXO INFORMACIONAL NA LEI DE INTERCEPTAÇÃO TELEFÔNICA E OS DESAFIOS DA PERSECUÇÃO PENAL

Artigo apresentado ao Departamento de Ciências Sociais Aplicadas como parte dos requisitos para obtenção do grau de Bacharel em Direito, no Curso de Graduação em Direito da UFERSA.

Orientador: Prof. Dr. Ulisses Levy Silvério dos Reis.

Mossoró/RN
2020

Lívia Andrade Albuquerque Valença

A PROTEÇÃO DO FLUXO INFORMACIONAL NA LEI DE INTERCEPTAÇÃO TELEFÔNICA E OS DESAFIOS DA PERSECUÇÃO PENAL

Artigo apresentado ao Departamento de Ciências Sociais Aplicadas como parte dos requisitos para obtenção do grau de Bacharel em Direito, no Curso de Graduação em Direito da UFERSA.

APROVADA EM: ____/____/____

BANCA EXAMINADORA

_____

Prof°. Dr. Ulisses Levy Silvério dos Reis (UFERSA)
Presidente

_____

Prof°. Dr. Luiz Felipe Monteiro Seixas (UFERSA)
Primeiro Membro

_____

Profª. Ms. Camila Jéssica Neres de Oliveira (UFERSA)
Segundo Membro

A PROTEÇÃO DO FLUXO INFORMACIONAL NA LEI DE INTERCEPTAÇÃO TELEFÔNICA E OS DESAFIOS DA PERSECUÇÃO PENAL

Lívia Andrade Albuquerque Valença[1]
Ulisses Levy Silvério dos Reis[2]

Resumo: A Constituição Federal de 1988, em seu art. 5º, XII, parte final, determina a inviolabilidade do sigilo de dados, exceto por ordem judicial, para fins de investigação criminal. A Lei n. 9.296, de 24 de julho de 1996, ao regular tal inciso, informa que não se admitirá a quebra do sigilo quando não houver indícios razoáveis da autoria ou participação em infração penal. Ocorre que, por decisão judicial, tem se permitido a quebra do sigilo quanto a informações sobre as pessoas que estiveram neste local e horário delimitados, mesmo que não estejam elas envolvidas com o delito em investigação. Tal possível contradição entre a regra legal e as decisões judiciais gera o questionamento: a quebra de sigilo de dados pessoais, em processos penais nos quais não se tem a identificação dos suspeitos do ilícito, é compatível com a Constituição? O estudo é relevante considerando o contexto brasileiro, no qual discursos violentos de persecução penal estão cada vez mais presentes, o que gera preocupações em termos de segurança jurídica. A pesquisa trabalhou com fontes diretas, analisando a normatividade de proteção à privacidade e aos dados pessoais no Brasil, com foco na Constituição Federal de 1988 e no Marco Civil da Internet, e indiretas, verificando as hipóteses que autorizam a quebra de sigilo de dados em sistemas de informática. O artigo foi dividido em três partes, em um primeiro momento, tratou-se da importância do requisito de existência de indícios razoáveis da autoria em infração penal para a quebra de sigilo. Em seguida, questionou-se a aplicação do Marco Civil da Internet como mecanismo de segurança para os indivíduos e para o processo penal. Por fim, foi analisado o caso Marielle Franco e Anderson Gomes. Foi possível concluir que as decisões judiciais que permitem a quebra de sigilo de dados pessoais sem prévia identificação dos suspeitos do ilícito é incompatível com a Constituição de 1988, sendo imprescindível a justa causa para tal quebra, pautada na realidade tecnológica, sem ferir o direito à privacidade e à proteção de dados pessoais. Pode-se inferir ainda pela necessidade de adequação legislativa pela criação de uma lei específica que regulamente as hipóteses de quebra de sigilo e quais os limites válidos.

Palavras-chave: Interceptação Telemática; Quebra de Sigilo; Proteção de dados; Persecução penal.

[1] Estudante do 11º período do Curso de Direito da Universidade Federal Rural do Semiárido (UFERSA), campus Mossoró/RN.
[2] Professor Adjunto C-1 da Universidade Federal Rural do Semiárido (UFERSA). Doutor em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal do Ceará (PPGD/UFC). É vice-líder do Grupo de Pesquisa em História do Constitucionalismo Brasileiro: a construção social da cidadania e a mudança constitucional no Brasil entre 1920 a 1988 (DGP/CNPq/UFERSA).

THE PROTECTION OF THE INFORMATIONAL FLOW IN THE LAW OF TELEPHONE INTERCEPTION AND THE CHALLENGES OF CRIMINAL PERSECUTION

Abstract: The Federal Constitution of 1988, in its art. 5, XII, final part, determines the inviolability of data privacy, except by court order, for the purposes of criminal investigation. Law 9,296, of July 24, 1996, when regulating such item, informs that the breach of confidentiality will not be admitted when there is no reasonable evidence of authorship or participation in a criminal offense. However, by judicial decision, the breach of confidentiality regarding information about people who have been in this place and time has been allowed, even if they are not involved with the crime under investigation. Such a possible contradiction between the legal rule and the judicial decisions raises the question: is the breach of confidentiality of personal data, in criminal proceedings in which there is no identification of suspected criminals, compatible with the Constitution? The study is relevant considering the Brazilian context, in which violent discourses of criminal prosecution are increasingly present, which raises concerns in terms of legal security. The research worked with direct sources, analyzing the norms for the protection of privacy and personal data in Brazil, focusing on the Federal Constitution of 1988 and the Civil Framework of the Internet, and indirect, verifying the hypotheses that authorize the breach of confidentiality of data in computer systems. The article was divided into three parts, at first, it dealt with the importance of the requirement of existence of reasonable evidence of authorship in criminal offense for breach of confidentiality. Then, the application of the Marco Civil da Internet was questioned as a security mechanism for individuals and for criminal proceedings. Finally, the case of Marielle Franco and Anderson Gomes was analyzed. It was possible to conclude that the judicial decisions that allow the breach of confidentiality of personal data without prior identification of the suspected criminals are incompatible with the 1988 Constitution, and the just cause for such breach, based on technological reality, is essential, without harming the right to privacy and protection of personal data. It can also be inferred by the need for legislative adaptation by creating a specific law, regulating the hypotheses of breach of confidentiality and which are the valid limits.

Keywords: Telematic Interception; Breach of Secrecy; Data protection; Criminal prosecution.

1 INTRODUÇÃO

A tecnologia tem transformado cada vez mais rápido as relações intersubjetivas, modificando, por conseguinte, as necessidades legislativas como um todo. A consequência disto é uma legislação que rapidamente se torna obsoleta, muitas vezes carente de efetividade, restando ao Judiciário a resolução de diversos conflitos a partir de categorias ambíguas como “proporcionalidade” e “razoabilidade”.

Nesse contexto, surge a possibilidade de o Estado se utilizar de dados pessoais, inclusive de localização, fornecidos pelos usuários a empresas de tecnologia para apuração de ocorrência de qualquer ilícito. Isso pode significar, por exemplo, que o Judiciário recorra à quebra de sigilo de dados de posse das empresas de tecnologia para fins de identificar os

endereços de Protocolos de Internet e, dessa maneira, chegar à possível identificação das pessoas que estavam localizadas nas proximidades em que o crime ocorreu, durante o período em que ele foi praticado.

A Constituição Federal de 1988, em seu art. 5º, XII, parte final, determina a inviolabilidade do sigilo de dados, exceto por ordem judicial para fins de investigação criminal. A Lei n. 9.296, de 24 de julho de 1996, informa que não se admitirá a interceptação de dados telemáticos quando não houver indícios razoáveis da autoria ou participação em infração penal. Dessa forma, a legislação veda a interceptação de dados telemáticos quando não se pode identificar previamente a identidade das pessoas envolvidas em determinado crime. A Lei n. 12.965, de 23 de abril de 2014 (também chamada de "Marco Civil da Internet"), por sua vez, disciplina o uso da internet no Brasil ao assegurar o direito à inviolabilidade da intimidade e da vida privada, a inviolabilidade do sigilo do fluxo de comunicações pela internet e a inviolabilidade do sigilo de comunicações privadas armazenadas, todos com uma ressalva: "salvo por ordem judicial, na forma da lei".

Todavia, não é isso o que se tem decidido nos casos em que a única informação que se tem é a do perímetro e do horário em que ocorrem os delitos. Por decisão judicial, tem se permitido a quebra do sigilo quanto a informações sobre as pessoas que estiveram no local e horário delimitados, mesmo que não estejam elas estas envolvidas com o delito em investigação.

Tal possível contradição entre a regra legal e as decisões judiciais gera o questionamento: a quebra do sigilo de dados pessoais, em procedimentos penais nos quais não se tem a identificação dos suspeitos do ilícito, é compatível com a Constituição? Desta pergunta infere-se três questões mais específicas: i) em quais medidas o requisito de existência de indícios razoáveis da autoria ou participação em infração penal são importantes, legalmente e materialmente, para a quebra de sigilo?; ii) Quais as consequências práticas na vida dos sujeitos envolvidos nesses processos?; iii) A aplicação do Marco Civil da Internet é um mecanismo de segurança suficiente para a proteção dos indivíduos e do processo penal?

O estudo é relevante considerando o contexto brasileiro, no qual discursos violentos de persecução penal estão cada vez mais presentes, o que gera preocupações em termos de segurança jurídica. As tecnologias de armazenamento de dados, por sua vez, estão em forte crescimento, viabilizando mecanismos práticos para as violações à intimidade dos titulares destes dados, mecanismos não imaginados na construção de leis como a Lei de Interceptação Telefônica (Lei n. 9.296/1996). Por se tratar de tema recente, não há uma unicidade de decisões, havendo uma pluralidade de opiniões e deliberações. Neste contexto, faz-se necessário que a

academia discuta tais temas a fim de que seja construído o conhecimento necessário para lidar com as demandas sociais reais.

A pesquisa trabalhou com fontes diretas e indiretas. Quanto às primeiras, foi analisada a normatividade de proteção à privacidade e aos dados pessoais no Brasil, com foco na Constituição Federal de 1988 e no Marco Civil da Internet. No mesmo passo, foram verificadas as hipóteses que autorizam a quebra de sigilo de dados em sistemas de informática ou telemática. Essa investigação foi realizada a partir da contextualização com a jurisprudência brasileira, com foco na atuação do Superior Tribunal de Justiça (STJ), e a partir da crítica literária.

O trabalho foi dividido em três sessões. A primeira tratará da importância do requisito de existência de indícios razoáveis da autoria ou participação em infração penal para a quebra de sigilo; a segunda questionará a aplicação do Marco Civil da Internet como mecanismo de segurança para os indivíduos e para o processo penal; por fim, será analisado o caso Marielle Franco e Anderson Gomes com o intuito de ilustrar as questões discutidas e vê-las sendo aplicadas na prática.

Valores e direitos humanos são violados constantemente sob o pretexto de condenar sujeitos, em sua maioria vulnerabilizados pela conjuntura social em que estão inseridos, prejudicando, inclusive, os direitos de terceiros não envolvidos. Este artigo pretende contribuir com a construção de ideias em prol da segurança da sociedade pautada na realidade tecnológica sem ferir o direito à privacidade e à proteção de dados pessoais.

2 A IMPORTÂNCIA DO REQUISITO DE EXISTÊNCIA DE INDÍCIOS RAZOÁVEIS DA AUTORIA OU PARTICIPAÇÃO EM INFRAÇÃO PENAL

O direito à inviolabilidade do sigilo de dados telemáticos está disposto na Constituição Federal de 1988, em seu art. 5º, XII, parte final, sendo considerado um direito fundamental. Os direitos fundamentais, além de normas base para outras, são normas reguladoras de relações jurídicas, de modo que a legislação deve segui-los e não o contrário.

O direito à privacidade possibilita ao indivíduo decidir o que deseja publicizar, de modo que este detém a autonomia exclusiva para decidir se outras pessoas terão acesso ou não ao conjunto de dados que se referirem a ele enquanto portador destes dados. Uma vez acessadas estas informações, sem a permissão do titular, tem-se a violação da privacidade.

A informação se conecta a uma série de fenômenos que cresceram em importância e complexidade de forma notável nas últimas décadas, se destacando pela maior facilidade de manipulação que tem adquirido ao longo do tempo, desde a coleta e tratamento até a

comunicação da informação. O aumento da capacidade de armazenamento e comunicação de informações é proporcional à variedade de formas pelas quais a informação pode ser apropriada ou utilizada (DONEDA, 2011).

Importa destacar que os direitos e garantias fundamentais são previstos pela Constituição Federal, mas não devem ser usados como um "escudo protetor" de práticas ilícitas para afastar a responsabilidade civil ou penal por ilicitudes.

Portanto, os direitos e garantias individuais não são absolutos, encontrando limites nos demais direitos também consagrados pela Constituição (LOPES, 2020). Caso contrário, a utilização indevida de direito fundamental em benefício próprio se chocaria com a garantia de exercício do direito de outrem. Nos casos em que os princípios de direitos fundamentais estão em conflito, busca-se a conciliação entre eles, conforme o caso concreto, sem que um deles tenha que ser totalmente excluído em face do outro.

Se tratando do direito à inviolabilidade de sigilo, é necessário o sopesamento entre os interesses do indivíduo portador das informações, da sociedade e do Estado. Ademais, o próprio inciso XII salvaguarda os casos estabelecidos por lei para fins de investigação criminal ou instrução processual penal, autorizados por ordem judicial.

Isso não significa que não sejam impostos limites ao Estado, considerando que este deve cumprir com suas finalidades, proporcionando segurança aos cidadãos, sem permitir que aquele que sofreu com o rompimento do sigilo com a quebra de dados tenha seu direito fundamental à intimidade violado.

Imprescindível, neste momento, diferenciar-se a interceptação de dados telemáticos da quebra de sigilo de dados telemáticos. O primeiro se trata da invasão de uma comunicação, da captação das informações no momento real e imediato em que elas ocorrem, por intermédio de gravações, escutas, acesso a dispositivos eletrônicos, entre outros. A quebra de sigilo de registros e dados, por sua vez, corresponde à obtenção de registros já existentes, como ligações já realizadas, dados cadastrais do assinante, número do endereço IP[3] do dispositivo utilizado, localização em que esteve, data, horário, duração do uso etc.

Muito embora exista essa diferença conceitual, é possível observar decisões judiciais que utilizam estes termos como sinônimos, como no caso do Recurso Extraordinário 418.416-8/SC, no qual se afirmou que, no caso, "não houve quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os

[3] O IP (*Internet Protocol*) é o protocolo da camada de rede da arquitetura TCP/IP responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores, permitindo que conexões e dispositivos sejam identificados a partir de uma sequência numérica própria.

dados, mediante prévia e fundamentada decisão judicial", cujo sentido das aspas é tão somente relacionar os assuntos como se fossem expressões equivalentes.

Outro exemplo de tal equivalência, bastante comum quando se trata deste assunto, são as decisões judiciais acerca da quebra de sigilo que se utilizam da Lei n. 9.296/1996, responsável por delimitar as hipóteses e formas de aplicação da possibilidade da interceptação de dados telemáticos. É o caso da decisão tomada no Mandado de Segurança 2240432.19.2018.8.26.0000, julgado pela 16ª Câmara de Direito Criminal do Tribunal de Justiça de São Paulo, que, mesmo deixando claro tratar-se de uma quebra de sigilo, ou seja, da obtenção de registros anteriormente existentes, baseia-se na Lei de Interceptação Telefônica para conceder a liminar. O mesmo comportamento se repete no Recurso em Mandado de Segurança 62.143/RJ (2019/0318252-3), no Recurso em Mandado de Segurança 61.302/RJ (2019/0199132-0), no Mandado de Segurança 59.716/RS (2018/0342755-1) e no Mandado de Segurança 61.419/SE (2019/0212818-0), todos julgados pelo Superior Tribunal de Justiça.

Esta equivalência, todavia, não é pacífica. Recentemente, o Ministro Luiz Fux, ao julgar o *Habeas Corpus* 167.720/SP, argumentou que a proteção contida no art. 5º, inciso XII, da Constituição se restringiria ao sigilo das comunicações telefônicas e telemáticas, não abrangendo os dados já armazenados em dispositivos eletrônicos. Ante essa assincronia de termos e conceitos, faz-se necessário analisar tanto a Lei de Interceptação Telefônica quanto o Marco Civil da Internet.

Começando pela Lei de Interceptação Telefônica, esta apresenta, em seu art. 2º, três hipóteses de vedação à interceptação de dados: i) quando o fato investigado constituir infração penal punível com pena de detenção; ii) quando a prova puder ser feita por outros meios disponíveis; e iii) quando não houver indícios razoáveis da autoria ou participação em infração penal. Desta conjuntura, pode-se questionar: em casos de crimes nos quais se tem apenas a localização e o horário de sua ocorrência, não havendo outro meio de obtenção de provas, com possibilidade de atribuição da pena de reclusão e não haja indícios razoáveis de autoria, é possível quebrar o sigilo dos dados?

Num primeiro momento, a resposta negativa se impõe. Todavia, imagine-se que, na apuração de um delito, os supostos autores estivessem se utilizando de *smartphones* conectados à internet com serviço de geolocalização e que estes dados estivessem disponíveis para uma empresa de tecnologia com grande capacidade de armazenamento. Estes dados seriam capazes de identificar os aparelhos e seus proprietários. Nesta particular situação, seria possível quebrar o sigilo de dados, requisitando à empresa telefônica a identificação das pessoas que estivessem

presentes em determinada circunferência, durante determinado horário, para fins de obtenção das provas de indícios razoáveis de autoria.

A Lei n. 9.296/1996 não definiu o significado de "indícios razoáveis", dando ampla margem interpretativa à autoridade jurisdicional. Avólio (2010, pp. 227) afirma que "nem precisaria a lei estabelecer tais requisitos para concessão da medida, pois difícil imaginar a concessão de obtenção de prova dessa natureza, sem observar um princípio de prova". Ocorre que, em 1996, no ano de criação da lei, sequer existiam *smartphones*. Em 2010, ano desta afirmação, provavelmente não se pensava na situação supracitada.

Para melhor ilustrar esta situação, observe-se o caso do assalto à empresa Prosegur, em Ribeirão Preto/SP. No dia 5 de julho de 2016, no bairro de Campo Eliseos, em Ribeirão Preto, interior de São Paulo, uma quadrilha com cerca de 40 criminosos armados invadiu a empresa de segurança e transporte de valores Prosegur. Na ocasião, foram estourados os transformadores de energia, deixando o bairro sem luz de maneira a conseguir acesso ao cofre do estabelecimento. Os criminosos conseguiram fugir levando consigo mais de R$ 51 milhões, tendo atirado em dois policiais, levando um deles ao falecimento.

A autoridade policial solicitou judicialmente uma quebra de sigilo telemático a fim de obter os dados de usuários de celular com contas ativas do Google, da Apple e da Microsoft de todas as pessoas que estiveram num raio de 500 metros da chácara, entre os dias 2 de julho e 5 de julho, das 13h às 19h, período em que o local era utilizado pelos criminosos.

Os dados requisitados pelas autoridades policiais foram a relação dos locais salvos pelos usuários nos aplicativos de mapa e GPS dos celulares, o histórico de localização e deslocamento nos últimos 30 dias, a atividade das respectivas contas nos últimos 30 dias, o IP dos aparelhos telefônicos, a data e hora dos acessos, a marca e o modelo dos celulares, o número telefônico do dispositivo, as fotos armazenadas nos últimos 30 dias nas plataformas de armazenamento de fotos e todas as senhas armazenadas no serviço passwords.google.com.

É importante destacar que, com este último pedido, os investigadores poderiam ter acesso a dados confidenciais de múltiplos serviços e plataformas não necessariamente operados pelo Google, como bancos, Receita Federal, laboratórios médicos e sites de compras online.

O pedido foi deferido de forma integral pela juíza em primeira instância, exatamente nos moldes apresentados pela autoridade policial. Segundo a magistrada, a quebra de sigilo de informações pessoais e dados telefônicos são legais e autorizadas pela Constituição. A intenção por trás desta decisão era a de investigar e identificar membros da organização criminosa, mas ela acabou afetando qualquer pessoa que transitou próximo ao local, inclusive advogados, que são protegidos por sigilo profissional com os clientes.

O argumento utilizado para tais quebras de sigilo em geral é de que, em alguns casos, se trata do único meio que a polícia e o aparato estatal possuem para tentar chegar no autor da infração penal.

O entendimento do STJ, presente nos Acórdãos citados anteriormente, é no sentido de que não deve ser feita uma interpretação extensiva do termo "indícios razoáveis", considerando que a ordem seria dirigida a um provedor de serviço de conexão ou aplicações de internet, o que não exigiria, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação. A explicação para tanto é que para a quebra de sigilo de dados armazenados, inclusive associada aos outros dados pessoais, não carrega a obrigatoriedade da indicação prévia das pessoas investigadas, quando, na verdade, é justamente essa a intenção da medida: a identificação dos envolvidos.

3 A APLICAÇÃO DO MARCO CIVIL DA INTERNET COMO MECANISMO DE SEGURANÇA PARA A PROTEÇÃO DOS INDIVÍDUOS E DO PROCESSO PENAL

Partindo do pressuposto de que a interceptação de dados telemáticos e a quebra do sigilo de dados telemáticos são mecanismos distintos, isso significaria dizer que a Lei de Interceptação Telefônica não se aplicaria aos casos de quebra de sigilo comentados, pois nestes as autoridade policiais solicitam os dados de identificação com base na localidade em que os possíveis autores dos crimes estiveram antes da obtenção destes dados, e não os dados instantâneos, como, por exemplo, onde tais autores estariam no presente momento da obtenção dos dados.

Dessa forma, restaria a delimitação da aplicação deste instrumento à Lei n. 12.965/2014, conhecida como Marco Civil da Internet. Considerada a lei uma solução aos crescentes questionamentos envolvendo violações de dados e comunicações que afetam a vida privada e a intimidade dos cidadãos, em sua elaboração, o legislador buscou respostas eficazes para disciplinar o uso das novas tecnologias de comunicação digitais, calcado nos princípios da universalidade, da neutralidade e da descentralização da rede mundial de computadores.

Ávila (2017) aduz que o conjunto de normas do Marco Civil da Internet destoa do texto constitucional ao permitir a violação das comunicações via internet, mesmo que por ordem judicial, nas hipóteses que a forma da lei estabelecer, uma vez que a Constituição só exclui o sigilo na hipótese de comunicação telefônica. Desta forma, o alcance da quebra de sigilo iria além da autorização constitucional.

A lei disciplina o uso da internet no Brasil atribuindo alguns princípios, dentre os quais destacam-se o princípio da proteção da privacidade e o princípio da proteção dos dados

pessoais, previstos em seu art. 3º, II e III. Dados pessoais, neste contexto, são entendidos como o dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa.

O Marco Civil da Internet ainda garante aos usuários da internet a inviolabilidade da intimidade e da vida privada, a inviolabilidade do sigilo do fluxo de suas comunicações pela internet e a inviolabilidade do sigilo de suas comunicações privadas armazenadas. Estes últimos, contudo, admitem exceção desde que por ordem judicial e na forma da lei.

No seu art. 22, a lei determina que a parte interessada na quebra dos sigilos poderá requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet com o propósito de formar conjunto probatório em processo judicial cível ou penal, instituindo como requisitos fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e período ao qual eles se referem.

Este dispositivo do Marco Civil da Internet estabilizou o entendimento já sedimentado a partir da leitura do art. 5º, XII, da Constituição, segundo o qual somente ordem judicial, necessária e proporcional, seria capaz de, excepcionalmente, afastar o sigilo de dados. Com isto, a autoridade judiciária se torna protetora da privacidade do indivíduo, tendo a missão de analisar o caso concreto e assim decidir pela quebra de sigilos.

O Decreto n. 8.771, de 11 de maio de 2016, responsável, entre outras coisas, por regulamentar o Marco Civil da Internet e apontar medidas para requisição de dados pela administração pública, em seu art. 11, § 3º, aduz que os pedidos de acesso a dados devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

No Marco Civil da Internet, diferentemente do trazido pela Lei de Interceptação Telefônica, não é substancial que haja indícios razoáveis de autoria, mas tão somente da ocorrência do ilícito. Não obstante, o decreto supracitado ordena a especificação dos indivíduos cujos dados estão sendo requeridos.

Ocorre que muitos dos pedidos de autoridades policiais para conseguir o acesso aos dados pessoais das pessoas envolvidas na investigação criminal são baseados no art. 10 do Marco Civil da Internet, que, em seu § 3º, informa que o disposto no *caput* (o dever de atender à preservação da intimidade na guarda e na disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas) não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação

e endereço pelas autoridades administrativas que detenham competência legal para a sua requisição.

Neste sentido, a interpretação de que as autoridades administrativas podem acessar os dados cadastrais independente da especificação dos indivíduos cujos dados estão sendo requeridos resulta na presunção de que todos são potenciais culpados.

Observe-se possível inconstitucionalidade no tocante ao descumprimento de outro direito fundamental: a presunção de inocência. É este direito que garante ao indivíduo a salvaguarda do direito à inviolabilidade de seus dados, de exigir uma decisão judicial fundamentada para a quebra de sua privacidade, deixando nas mãos das autoridades investigativas a obrigação de apresentar em juízo a fundamentação contrária. Para adentrar a esfera íntima, deverá o Estado demonstrar a necessidade e proporcionalidade da medida à autoridade judiciária competente. Só a partir da decisão judicial fundamentada poderá se quebrar o sigilo de dados. Antes disso, todo indivíduo tem o direito de salvaguarda de suas informações, que não podem ser devassadas como se fossem suspeitas desde o princípio.

A indispensabilidade de decisão judicial para a quebra de sigilo de dados se mostra de suma importância como obstáculo ao arbítrio do Estado. Isto porque a presunção de inocência é uma norma de juízo, manifestando-se em todas as decisões proferidas na persecução penal, qualificando e legitimando o ato.

A 16ª Câmara de Direito Criminal do Tribunal de Justiça de São Paulo, ao apreciar o Mandado de Segurança 2212203-49.2018.8.26.0000, de forma unânime, anulou decisão de primeiro grau que determinava o fornecimento do histórico de localização e "todos os trajetos efetuados por todos os celulares" que tenham sido identificados num raio de 200 metros de cinco locais diferentes do município de Catanduvas/SP, num período de duas horas.

Conforme o relator, a ordem recebida pelo Google é nula de pleno direito em razão de não ser lícito impor medida constritiva e excepcional a um número expressivo e indeterminado de usuários. A excepcionalidade e restritividade da medida, segundo o Desembargador, deve se pautar na indicação e individualização das pessoas objeto da quebra de sigilo, considerando a repercussão na vida de inúmeras pessoas que residem em conjuntos habitacionais, que passaram por uma rodovia estadual ou que estavam a 200 metros de pontos pré-determinados, concluindo que a ordem é genérica e exploratória e, portanto, viola exigência legal de individualização dos alvos de quebra de sigilo.

A 7ª Câmara Criminal do Tribunal de Justiça do Rio de Janeiro, nos autos do Mandado de Segurança 0038839-36.2016.8.19.0000, afirmou que sustentar que a quebra de sigilo de dados sem a identificação individualizada dos investigados poderia ser viável a tal ponto de

permitir a identificação de personagens ligados ao narcotráfico é agir em contrariedade à lei para apenas satisfazer a falta de estrutura na prática daqueles que exercem a difícil tarefa de investigar crimes.

Considerando tratar-se de uma discussão que permeia a proteção de dados, mostra-se necessário a observação quanto à não aplicação da Lei n. 13.709, de 14 de agosto de 2018 (a chamada "Lei Geral de Proteção de Dados – LGPD") à matéria. Isto porque o próprio legislador optou por não contemplar o tratamento de dados para segurança pública e investigação criminal no âmbito de aplicação da LGPD, estabelecendo expressamente a necessidade de aprovação de lei específica para esse tema por meio do seu art. 4º, *caput* e inciso III, "a" e "d", e § 1º.

Esta medida se trata de uma ordem legal para legislar sobre a matéria, a partir da constatação de que o assunto está sujeito a reflexões específicas sobre o uso de dados pessoais e que expressa reivindicação da sociedade e das autoridades competentes para regulação do tema, surgida no processo de debate da própria LGPD. Diante disto, o Ministro Nefi Cordeiro, do Superior Tribunal de Justiça, entregou ao Presidente da Câmara dos Deputados, em 05 de novembro de 2020, um anteprojeto de lei que trata da utilização de dados de segurança pública.

O anteprojeto, estruturado em 12 capítulos, com 68 artigos, está em trâmite na Câmara e conta com um capítulo exclusivo para regulamentar o tratamento de dados pessoais para fins penais.

4 O CASO MARIELLE FRANCO E ANDERSON GOMES

O caso de Marielle Franco e Anderson Gomes, executados brutalmente em 14 de março de 2018 após participarem de um evento na Casa das Pretas, no bairro da Lapa, no centro do Rio de Janeiro/RJ, tomou repercussão internacional pela frieza do assassinato que ganhou bojo político pelo papel de destaque que Marielle vinha ganhando. A vereadora, de origem periférica, era lésbica, ativista de direitos humanos e vinha denunciando a atuação truculenta da polícia em favelas do Rio de Janeiro/RJ, num momento em que começava a intervenção federal com apoio dos militares na cidade.

Durante a investigação deste crime, as autoridades policiais solicitaram a quebra do sigilo de dados para fins de identificação das pessoas nele envolvidas. No acórdão do Recurso em Mandado de Segurança 62.143/RJ (2019/0318252-3), interposto perante o STJ pelo Google Brasil Internet Ltda. e Google LLC contra a decisão proferida pelo Tribunal de Justiça do Rio de Janeiro, foi impugnada a decisão do Juiz de Direito da 4ª Vara Criminal da Comarca do Rio de Janeiro/RJ, que autorizou a identificação dos usuários de aplicativos de um conjunto não

identificado de pessoas tão somente pela circunstância aleatória de haverem transitado, em certo lapso de tempo, por determinadas coordenadas geográficas no Município do Rio de Janeiro/RJ.

O Google argumentou que a determinação judicial perdeu o objeto, pois houve evolução da investigação e a identificação dos suspeitos dos crimes. Acrescentou também que o ordenamento jurídico brasileiro não admite quebras de sigilo e interceptações genéricas, desprovidas de individualização razoável dos indivíduos afetados e das respectivas fundamentações, e aduziram que a premissa para quebras de sigilo, no sistema jurídico, é a existência e demonstração de indícios concretos de envolvimento de determinada pessoa na prática de crimes e que não há previsão legal para quebra de sigilo com base em meras coordenadas geográficas.

A empresa apontou que a quebra de sigilo é medida excepcional e que só pode ser justificada pela existência de indícios concretos de atividade ilícita por parte do alvo delimitado que devem estar claros em decisão judicial fundamentada, invocando os arts. 5º, X e XII, e 93, X, da Constituição, o art. 2º da Lei n. 9.296/1996, o art. 22 do Marco Civil da Internet, o art. 11 do Decreto n. 8.771/2016 e a Resolução CNJ n. 59/2008.

No recurso, foi aduzida a invalidez da ordem de quebra de sigilo por ela não oferecer a individualização dos alvos contra os quais existem os indícios de autoria e participação. Para que fossem preenchidos os requisitos de validade compatível com a ordem jurídica brasileira, deveriam necessariamente ser informado o identificador dos alvos, fosse nome de usuário, e-mail, IMEI, URL do perfil, entre outros.

Além do mais, argumentou-se ser inadmissível que o direito à privacidade de pessoas inocentes seja afastado sem justa causa, de modo que não pode haver quebra de sigilo com base apenas em área geográfica e lapso de tempo, sob risco de tornar garantias constitucionais e requisitos legais escusáveis de qualquer força normativa. Segundo o Google, a determinação judicial transformaria cada *smartphone* em um dispositivo de vigilância pessoal invasivo à disposição ao Estado de forma remota.

Ao final, alegaram a inobservância ao princípio da proporcionalidade, eis que a quebra do sigilo não ofereceu garantias de que levará aos autores do delito investigado e não há garantia de confiabilidade nos dados de geolocalização a serem pesquisados, além de ser desnecessária, por haver diligências alternativas, e desproporcional em sentido estrito, por aceitar o dano colateral de quebrar o sigilo de inocentes, assumindo que a medida extrema seria justificável pela possibilidade apenas eventual de se obter alguma pista sobre aqueles que teriam envolvimento nos crimes investigados.

O Ministério Público, instado a se manifestar, alegou que os direitos fundamentais não são absolutos, devendo ser ponderados diante de outros direitos e interesses de igual ou semelhante importância e que o acolhimento do recurso interposto pela Google representaria a instituição do "Paraíso do Crime". O *parquet* pontuou que a própria redação do inciso XII, do art. 5°, da Constituição prevê a possibilidade da relativização do direito ao sigilo de dados por meio de ordem judicial. Frisou ainda a relevância e complexidade da investigação criminal que deu causa à quebra de sigilo, cujo objeto é o assassinato da vereadora Marielle Franco e de seu motorista, Anderson Gomes, caso de notória repercussão social.

Segundo o Ministério Público, o motivo desta decisão se refere à circunstância de o veículo utilizado no assassinato não ter sido apreendido após o crime, ocorrido em 14 de março de 2018. Argumentou que, por tratar-se da realização de atividade investigatória, esta não poderia ser obstada ou inviabilizada, sob pena de prevalecer a criminalidade. Seria também importante promover a identificação da pessoa que, meses após o crime, se encontrava em poder do carro clonado e, para tanto, a investigação traçou um polígono das coordenadas do local em que o veículo foi visto, naquela data específica, em um lapso temporal de 15 minutos.

Quanto à alegação de desobediência aos ditames da Lei n. 12.965/2014 (Marco Civil da Internet), destacou o órgão que a própria legislação prevê a possibilidade do afastamento da proteção do direito à privacidade diante de direitos e interesses de igual relevância.

O Ministro Relator, Rogério Schietti Cruz, ao destacar o embate entre o direito à privacidade dos indivíduos e o interesse público na atividade de persecução penal e de segurança pública, afastou a preliminar de perda de objeto da decisão que determinou a quebra do sigilo de dados considerando que as investigações continuam em andamento. Reconheceu que o sigilo é expressão de um direito fundamental de alta relevância ligado à personalidade, mas pontuou que a doutrina e a jurisprudência compreendem que não se trata de um direito absoluto, admitindo-se a sua restrição, quando imprescindível para o interesse público.

Em seu voto, Cruz destaca que a decisão se refere a dados estáticos, configurando quebra de sigilo de dados informáticos, e não de interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o destinatário dela.

A justificativa é no sentido de que não há como dar interpretação extensiva aos dispositivos da Lei de Interceptação Telemática porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é prevista no Marco Civil da Internet, o qual não prevê, entre os requisitos que estabelece para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da

autoria) possa ser realizada por outros meios. Por fim, o Ministro negou provimento ao recurso do Google.

Apenas o Ministro Sebastião Reis Júnior divergiu do voto supracitado, esclarecendo que, em um primeiro momento, realmente não há a identificação pessoal do usuário; todavia, é evidente que tal determinação busca essa identificação ao final, caso contrário não teria razão de ser. Considerando o princípio constitucional que protege a privacidade, bem como o disposto no art. 11, § 3º, do Decreto n. 8.771/2016, que veda pedidos genéricos, ele entendeu pela ilegalidade da decisão levando em conta a não apresentação de justificativa suficiente quanto à extensão das informações solicitadas.

O caso demonstra a divergência ainda presente no cenário judiciário e pode ser um marco para outros similares, pois o foco da investigação não é a interceptação das conversas entre os criminosos, mas sim o cruzamento eficaz de dados e metadados obtidos.

Da análise destas decisões, verifica-se que a discussão sobre a inexistência de direitos absolutos recai em situações excepcionais em que o comportamento de algumas pessoas afeta os direitos de outrem. “Interesse público”, “interesse social” e “bem da comunidade” são termos frequentes na justificativa de restrições a direitos fundamentais e configuram conceitos jurídicos indeterminados, sempre abertos a alguma margem de discricionariedade na sua concretização pelo operador do direito.

A posição expressa pelo STJ no caso Marielle Franco e Anderson Gomes, sobre razões de interesse público ou mesmo exigências derivadas do princípio da convivência das liberdades, confirma essa proposição e demonstra que sua interpretação pode ser variável conforme o regime político adotado em um Estado, ou conforme o momento político e institucional vivido no país. Quanto às restrições à privacidade, verifica-se que essa situação que dá margem a alguma subjetividade do intérprete é frequentemente utilizada como justificativa para invadir a privacidade e a intimidade dos cidadãos por meio do monitoramento da rede e de e-mails pessoais.

5 CONCLUSÃO

No presente artigo, o art. 5º, XII, da Constituição foi analisado em correlação com a Lei n. 9.296/1996 e a Lei n. 12.965/ visando problematizar seu confronto quanto à compatibilidade constitucional da quebra de sigilo de dados pessoais em processos penais nos quais não se tem a identificação dos suspeitos do ilícito.

O aumento da capacidade de armazenamento e a maior facilidade de manipulação dos dados, resultado do avanço tecnológico, propicia o aumento das possibilidades de apropriação de informações e consequentes violações à privacidade.

Apesar de a doutrina diferenciar a interceptação de dados da quebra de sigilo de dados, a Lei de Interceptação Telefônica é frequentemente aplicada a casos de quebra de sigilo, com a interpretação restritiva do termo "indícios razoáveis", de modo que não se exige, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação.

O avanço legislativo é evidente ao observar-se o fato de o Estado ter elaborado, de forma colaborativa com a sociedade civil, a Lei 12.965/2014. Ao criar o Marco Civil da Internet, o Poder Público estabeleceu o aparato legal de implementar medida necessária à concretização do direito à privacidade. Todavia, por não se tratar de texto específico mais detalhado, ainda há margens para interpretações que põe em xeque a importância da inviolabilidade de sigilo.

Nesse cenário de rápidos avanços tecnológicos e de ausência de regulamentação específica sobre o tema, existe uma assimetria muito grande de poder entre o Estado e o cidadão, na qual os indivíduos são a parte vulnerável. O titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de privacidade, suas liberdades individuais e até a observância do devido processo legal.

Das decisões analisadas, verifica-se a forte presença do argumento de inexistência de direitos absolutos, trazendo consigo expressões como "interesse público", "interesse social" e "bem da comunidade", conceitos abertos à discricionariedade na sua concretização pelo operador do direito. A posição expressa pelo STJ no caso Marielle Franco e Anderson Gomes reafirma essa premissa e demonstra que sua interpretação pode ser variável conforme o regime político adotado em um Estado, ou conforme o momento político e institucional vivido pelo país.

O atropelo de garantias processuais não pode ser justificado pela busca pela rápida elucidação do fato criminoso, uma vez que se insere dentre as finalidades do processo penal a instrumentalização da máxima eficácia dos direitos e garantias fundamentais, especialmente da liberdade individual.

Em que pese o Estado ter legislado para assegurar a não interferência de terceiros na vida privada do cidadão, há, ainda, a necessidade de regulamentação de aspectos da privacidade na rede na esfera penal. Desse modo, resta comprovada a necessidade de iniciativas estatais para tutelar o direito à privacidade não apenas em face do Estado, mas também no tocante à

coletividade, como a iniciativa citada do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal.

6 REFERÊNCIAS

AVILA, Ana Paula Oliveira; WOLOSZYN, André Luís. A tutela jurídica da privacidade e do sigilo na era digital. Revista de Investigações Constitucionais, São Paulo, v. 4, n. 3, p. 167-200, dez. 2017. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=6132344. Acesso em: 30 nov. 2020

AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas:** Interceptações Telefônicas, ambientais e gravações clandestinas. 4. ed. São Paulo: Revista dos Tribunais, 2010.

BONDE, Tais Marcela. **Quebra de Sigilo:** a (des)necessidade de autorização judicial para acessar o conteúdo de aparelho celular apreendido. 2018. 59 f. TCC (Graduação) - Curso de Direito, Fepesmig, Três Pontas, 2018. Disponível em: http://repositorio.unis.edu.br/handle/prefix/822. Acesso em: 30 nov. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF, out. 1988.

BRASIL. Decreto n. 8.771, de 11 de maio de 2016. **Regulamenta a Lei nº 12.965, de 23 de abril de 2014.** Brasília, DF, jul. 2014.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasília, DF, abr. 2014.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Brasília, DF, ago. 2018.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.** Brasília, DF, jul. 1996.

CASTELLS, Manuel. **A Sociedade em Rede.** Tradução de Roneide Venancio Majer. – 19ª edição, revista e ampliada. – Rio de Janeiro/São Paulo: Paz e Terra, 2018.

DONEDA, D. (2011). A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL],** 12(2), 91-108. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 02 dez. 2020.

FARES, Mohamad Hassan. **Quebra de sigilo telemático.** 2018. 48 f. TCC (Graduação) - Curso de Direito, Universidade Presbiteriana Mackenzie, São Paulo, 2019. Disponível em: http://dspace.mackenzie.br/handle/10899/20154. Acesso em: 30 nov. 2020.

JOTA. **Juízes ordenam quebra coletiva de sigilo de dados com base em localização.** Por Alexandre Leoratti e Kalleo Coura. 27/05/2019, às 08h21. Atualizado em 27/05/2019, às 19h53. Disponível em: https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-

sigilo-de-dados-com-base-em-localizacao-27052019. Acesso em: 30 nov. 2020.

LOPES, Guilherme Araujo. **A FLEXIBILIZAÇÃO DOS DIREITOS FUNDAMENTAIS EM TEMPOS DE PANDEMIA – NENHUM DIREITO É ABSOLUTO**. Revolução na Ciência, Presidente Prudente, v. 16, n. 16, p. 1-11, set. 2020. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/8730/67650144. Acesso em: 30 nov. 2020.

PINTO, Felipe Martins; GUIMARÃES, Johnny Wilson Batista. O Direito à Privacidade e o Sigilo de Dados na Internet. **Revista da Faculdade de Direito da UFMG,** n. 69, p. 201-219, 10 fev. 2017. DOI: http://dx.doi.org/10.12818/p.0304-2340.2016v69p201. Acesso em: 01 dez. 2020.

SHIRAMA, Paula Martinez. **A Inviolabilidade do Direito à Intimidade na Quebra do Sigilo de Dados.** 2019. 78 f. TCC (Graduação) - Curso de Direito, Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente, Presidente Prudente, 2019. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/8282/67649371. Acesso em: 30 nov. 2020.

VILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais,** v. 4, n. 3, pp. 167-200, 2017. DOI: http://dx.doi.org/10.5380/rinc.v4i3.51295. Acesso em: 01 dez. 2020.