REVISTA
BRASILEIRA DE DIREITO

A observância do princípio da proporcionalidade no direito comparado quanto à interceptação de dados digitais

The observance of the principle of proportionality in comparative law on digital data interception

Matheus Arcangelo Fedato(1); Luiz Fernando Kazmierczak(2)

1 Mestrando em Ciência Jurídica pela Universidade Estadual do Norte do Paraná (UENP). Graduado em Direito pela Universidade Estadual do Norte do Paraná (UENP). E-mail: matheus.fedato@outlook.com
2 Doutor em Direito Penal pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Professor e Coordenador Adjunto do Curso de Direito nas Faculdades Integradas de Ourinhos (FIO) e Professor do Curso de Direito e do Programa de Pós-Graduação em Ciência Jurídica na Universidade Estadual do Norte do Paraná (UENP). E-mail: lfkaz@uenp.edu.br

Revista Brasileira de Direito, Passo Fundo, vol. 13, n. 3, p. 539-558, Set.-Dez., 2017 - ISSN 2238-0604
[Received/Recebido: Jul. 15, 2017; Accepted/Aceito: Dez. 12, 2017]
DOI: https://doi.org/10.18256/2238-0604.2017.v13i3.2038

Como citar este artigo / How to cite item: clique aqui!/click here!

Resumo

O artigo se propõe a analisar como o princípio da proporcionalidade está sendo utilizado no contexto das interceptações informáticas, estando o tema ligado à vigilância digital para a garantia da segurança pública e a proteção da privacidade. A análise se dá pela observância de como ordenamentos jurídicos estrangeiros (EUA, Alemanha, Portugal) tratam a matéria, tendo em vista os programas de interceptação americanos e sua declarada guerra ao terrorismo, a jurisprudência alemã e a sua visão de proporcionalidade e Portugal pela regulamentação do tema por determinação da União Europeia. Constatou-se que a proporcionalidade tem sido utilizada como modo de balizar o conflito de interesses gerados pela colisão dos direitos fundamentais. A preservação da privacidade mostrou-se privilegiada, restando, como exceção, os programas de espionagem do governo norte-americano. Para atingir o objetivo do estudo, foi utilizado o método dedutivo, além de meios de pesquisa eletrônicos e bibliográficos.

Palavras-chave: Princípio da Proporcionalidade. Colisão de Direitos. Segurança Pública. Privacidade. Interceptação de dados.

Abstract

The article proposes to analyze how the principle of proportionality is being used in the context of computer intercepts, linked the subject to the digital surveillance to guarantee public safety and the privacy protection. The analysis is based on observance of how foreign legal systems (USA, Germany, Portugal) deal with the matter, because of the American interception programs and their declaration of war on terrorism, the German jurisprudence and their view of proportionality and Portugal by regulating the subject by determination of the European Union. It has been observed that proportionality has been used as a means of assessing the conflict of interests generated by the collision of fundamental rights. The preservation of privacy has been privileged, with the exception of the espionage programs of the US government. To reach the study objective, the deductive method was used, as well as electronic and bibliographic research resources.

Keywords: Principle of Proportionality. Collision of Rights. Public Safety. Privacy. Data Interception.

1 Introdução

A temática do trabalho consiste na vigilância da transmissão de dados digitais, notadamente por meio da interceptação informática, e a utilização da proporcionalidade quando da adoção de medidas tendentes à violação da privacidade, buscando observar o tratamento dispensado à matéria por ordenamentos estrangeiros. Primeiramente, trabalha-se com o paradoxo existente entre a garantia da segurança pública e a garantia da privacidade, mostrando a possível colisão de direitos fundamentais e a importância da utilização do princípio da proporcionalidade, elaborando-se hipóteses para a solução do conflito.

Posteriormente, inicia-se a análise de direito comparado com a abordagem dada pelos Estados Unidos da América ao tema, analisando-se seus programas de governo, que, sob o manto da proteção contra o terrorismo, podem estar violando direitos fundamentais. Após, colocam-se em tela o direito alemão e a jurisprudência de seu Tribunal Constitucional no que tange a colisão de direitos fundamentais, haja vista ser essa Corte que primeiramente racionalizou o princípio da proporcionalidade. Ao final, estuda-se a diretiva 24/2006 da União Europeia, a qual tem extrema importância para o tema, e que pode ser considerada em correlação com a Lei nº 9.296/96, pois regulamenta a investigação em meios digitais para prevenção de crimes.

A problemática relaciona-se com o conflito de direitos fundamentais e a necessidade de se buscar respostas para sua solução. A proteção da privacidade e a prevenção de delitos ocasionam um impasse que merece atenção por parte do Direito. Tal estudo torna-se necessário pela novidade e complexidade do tema, sendo de grande valia para a pesquisa a análise do tratamento jurídico dado por outros países. A pesquisa objetiva analisar o conflito existente entre a segurança pública e a privacidade na modernidade, focando no âmbito da interceptação de dados digitais, e a necessidade da utilização da proporcionalidade, buscando observar como o Direito dos Estados Unidos da América, da Alemanha, de Portugal e da União Europeia lidam com a matéria.

2 Por uma efetiva garantia de direitos fundamentais: o paradoxo entre segurança e privacidade na modernidade

O trabalho pauta-se pelo paradoxo que ocorre entre a garantia da segurança pública e a preservação da privacidade na modernidade. Sob um viés sociológico, ambas estão em atrito e são de difícil conciliação, principalmente nos dias atuais, em que todos estão conectados e correm o risco de terem suas vidas privadas violadas. Assim,

> [...] a liberdade e a segurança, ambas igualmente urgentes e indispensáveis, são difíceis de conciliar sem atrito – e atrito considerável na maior parte do tempo. Estas duas qualidades são, ao mesmo tempo, complementares e incompatíveis; a chance de que entrem em conflito sempre foi e sempre será tão grande quanto à necessidade de sua conciliação. Embora muitas formas de união humana tenham sido tentadas no curso da história, nenhuma logrou encontrar solução perfeita [...][1]

Com o advento da "Era da internet", muitas coisas mudaram, principalmente o modo como se dão as relações entre as pessoas. Tudo é instantâneo, rápido, ágil, não se pode esperar, não há tempo para aguardar resposta. Tudo é extremamente fácil, e essa característica estimula o indivíduo a cada vez mais utilizar os meios digitais, haja vista que a sua rede de amizades lá se encontra, seja para conversar, postar, curtir ou comentar.

> [...] é importante compreender todo o mecanismo de funcionamento das novas tecnologias de comunicação, entre elas a internet, bem como sua evolução num cenário de convergência, uma vez que o Direito é resultado do conjunto comportamento e linguagem. Só com essa compreensão é que podemos fazer leis, aplicá-las e dar soluções ao caso concreto.[2]

Percebe-se que algo extraordinário está ao alcance dos usuários, os quais gradativamente aumentaram a possibilidade de expressar sua liberdade de opinião. O que antes era de conhecimento apenas pessoal, transforma-se em algo global, em que qualquer um, com acesso à internet, pode, com a devida permissão, tomar ciência e até interagir com o ocorrido. A comunicação está muito mais intensa do que era. Há milhões de pessoas se comunicando todos os dias através dos mais diferentes meios disponíveis, seja no celular, *tablet, smartphone*, computador, seja no *notebook*. A população está adquirindo o hábito de viver em função do meio digital, tornando o fluxo de informações gigantesco.

O modo como se vivia antigamente mudou, não se exige mais a *presencialidade*, basta apenas estar online para que o contato *humano* ocorra. Nos ensinamentos do sociólogo polonês Zygmunt Bauman, o que é ser moderno "passou a significar, como significa hoje em dia, ser incapaz de parar e ainda menos de ficar parado. Movemo-nos e continuaremos a nos mover [...] por causa da impossibilidade de atingir a satisfação". [3]

1 BAUMAN, Zygmunt. *Comunidade:* a busca por segurança no mundo atual. Trad. Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2003. p. 24.

2 PINHEIRO, Patricia Peck. *Direito Digital.* 5. ed. rev. atual. ampl. São Paulo: Saraiva, 2013. p. 65.

3 BAUMAN, Zygmunt. *Modernidade Líquida*. Trad. Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001. p. 37.

Desse modo a sociedade vive uma mudança profunda quanto ao modo de se relacionar de seus indivíduos. Criou-se certa dependência do mundo digital. A internet possibilita que pessoas que estejam a milhares de quilômetros de distância se comuniquem. Instantaneamente um vídeo pode ser acessado por várias pessoas em diversos lugares do mundo ao mesmo tempo. E isso tudo acontece apenas com o acesso à rede.

Um fato que acontece por meios digitais e que desperta o interesse do Direito é a conversação pelo uso de aplicativos de comunicação como *WhatsApp*; *Messenger*; *Skype*; *Viber*; *Telegram*, dentre outros. Claro que não interessa para a ciência do Direito a fiscalização de conversas pessoais comuns, mas as que demonstrem real potencial ofensivo à paz social e à vida das pessoas.

Pelas trocas de mensagens, usuários acabam por revelar muitas de suas intenções, pois se sentem protegidos por estarem utilizando um aparelho eletrônico. Algumas vezes essas atitudes são praticadas por pessoas que têm o intuito de vir a cometer crimes e que se comunicam por meio desses aplicativos de troca de mensagens. Estas podem passar informações confidenciais aos outros usuários, deixando registrados possíveis alvos de ataques terroristas, locais de encontro para realização de outros crimes, nomes e endereços de criminosos etc. É sabido que uma das funções do Direito é a preventiva. De modo que se fosse possível prever todos os crimes antes de ocorrer, viver-se-ia em um estado de paz social. Conforme Sérgio Cavalieri Filho[4],

> O conflito gera o litígio e este, por sua vez, quebra o equilíbrio e a paz social. A sociedade não tolera o estado litigioso, porque necessita de ordem, tranquilidade, equilíbrio em suas relações. Por isso, tudo faz para evitar ou prevenir o conflito, e aí está a primeira e principal função social do Direito - prevenir conflitos: evitar, tanto quanto possível, a colisão de interesses.

Entretanto, para que a referida proteção seja feita, pode ser necessário que a intimidade seja mitigada. O direito fundamental à privacidade está prescrito em nossa Constituição, sendo importantíssimo dentro do Estado Democrático de Direito. Em busca da prevenção, estar-se-ia abrindo mão da vida íntima das pessoas, daquilo que para cada um possui valor imensurável. Assim, faz-se necessária uma análise precisa de cada preceito posto em questionamento para que o resultado seja o mais "justo" possível, não preterindo um ao outro, não menosprezando um pelo outro, mas proporcionando cada um de maneira equitativa.

O conflito entre a privacidade e a segurança pública na modernidade[5] e seus

4 CAVALIERI FILHO, Sérgio. *Programa de Sociologia Jurídica*. Rio de Janeiro: Forense, 2007. p. 15.

5 "Esse é o paradoxo de nosso mundo saturado de dispositivos de vigilância, quaisquer que sejam seus pretensos propósitos: de um lado, estamos mais protegidos da insegurança que qualquer geração anterior; de outro, porém, nenhuma geração anterior, pré-eletrônica, vivenciou os sentimentos de insegurança como experiência de todos os dias (e de todas as noites)". BAUMAN, Zygmunt. *Vigilância Líquida*: diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

reflexos jurídicos é extremamente relevante, sendo necessário encontrar uma solução adequada para tal impasse. Não se tornando possível a garantia de um sem que o outro seja afetado, ou necessariamente afetando um na medida em que o outro seja garantido, indaga-se qual seria a melhor maneira de conseguir harmonizar as divergências de uma forma a não exaltar excessivamente um em detrimento do outro.

Dentre as possíveis soluções para o conflito, destaca-se a teoria da proporcionalidade, apresentada, principalmente, por Robert Alexy[6] e pelo Tribunal Constitucional Alemão (*Bundesverfassungsgericht*), e que demonstra uma capacidade de resolução de conflitos que envolvem direitos fundamentais, por tentar, racionalmente, elaborar uma decisão que leve em conta a adequação e a necessidade da medida tomada, bem como o sopesamento dos interesses e das medidas pela proporcionalidade em sentido estrito. Nessa linha, toma-se por base o caso concreto, estabelecendo relações de precedências condicionadas consistes na fixação de condições sob as quais um princípio tem precedência em face de outro.[7]

Nesse sentido, "o Princípio da Proporcionalidade é considerado um dos principais temas da interpretação dos direitos constitucionais"[8]. Assim, no que se refere às interceptações informáticas[9] (ou de dados digitais) e a decisão que as autoriza, a utilização do princípio da proporcionalidade mostra-se inevitável para a devida garantia e proteção dos direitos fundamentais envolvidos. Dessa forma, preserva-se

> […] um *núcleo essencial de direitos fundamentais* (inadmissibilidade da prova ilícita e dever de fundamentação das decisões judiciais), com perfeita *compatibilização com as disposições normativas processuais*, de índole infraconstitucional, considerando as especificidades do caso.[10]

6 ALEXY, Robert. *Teoria dos direitos fundamentais*. 2. ed. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2012.

7 Ibidem. p. 96.

8 MORAIS, Fausto Santos de; ZOLET, Lucas. Constitutional rights expansion and contributions from Robert Alexy's theory / A expansão dos direitos fundamentais e a contribuição teórica de Robert Alexy. *Revista Brasileira de Direito*, Passo Fundo, v. 12, n. 2, p. 127-136, dez. 2016. ISSN 2238-0604. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/1505/1006>. Acesso em: 24 mai. 2017. doi: http://dx.doi.org/10.18256/2238-0604/revistadedireito.v12n2p127-136. p. 132. Tradução nossa.

9 No Brasil as interceptações informáticas são reguladas pela Lei nº 9.296/96, que regulamentou o inciso XII, parte final, do art. 5° da Constituição Federal. Para um visão mais aprofundada da lei: STRECK, Lenio Luiz. *As Interceptações Telefônicas e os Direitos Fundamentais*: Constituição, Cidadania e Violência: A Lei 9.296/96 e seus reflexos penais e processuais. Revista e Ampliada. 2. ed. Porto Alegre: Livraria do Advogado, 2001.

10 DA SILVA, Eliezer Gomes; GIACOIA, Gilberto. Provas lícitas não repetíveis, autorizadas por decisões com deficiência de fundamentação: nulidade e inadmissibilidade da prova, nas interceptações telefônicas, e o necessário emprego da técnica de ponderação. In: *Anais do XXIV Congresso Nacional do CONPEDI - UFMG/FUMEC/Dom Helder Câmara – Processo Penal e Constituição*. Florianópolis: CONPEDI, 2015. p. 279.

Pois, no contexto das interceptações informáticas, está, justamente, a divergência que ocorre entre os ideais de preservação da privacidade ou da segurança pública. Dessa forma, entende-se ser o modo mais razoável para a resolução do paradoxo apresentado à utilização do princípio da proporcionalidade, pois este visa justamente à harmonização de direitos fundamentais quando em colisão.

É sempre "necessária uma fundamentação intersubjetivamente controlável, não basta somente identificar os valores em jogo, mas construir e lançar mão de critérios que permitam aplicá-los racionalmente"[11]. A utilização da proporcionalidade respalda o dever de fundamentação das decisões judiciais, sob pena de nulidade, conforme previsto pela Constituição Federal, em seu artigo 93, IX[12].

A fim de demonstrar a necessidade da correta aplicação do princípio da proporcionalidade, torna-se imperioso colacionar uma decisão do Supremo Tribunal Federal, a qual, baseada nos fundamentos do Tribunal de Justiça do Estado de São Paulo, considerou legal a duração das interceptações telefônicas por 30 dias, pois, no caso em tela, privilegiou-se a garantia da segurança pública em detrimento da privacidade.

Assim, a decisão do Habeas Corpus nº 439.764.3/3 do TJ/SP, de relatoria do desembargador Péricles Piza, que embasou o voto do Ministro Gilmar Mendes no RHC 88.371, emanou que, pelo princípio da proporcionalidade, no caso objeto de julgamento, "o direito à segurança, à proteção à vida [...] não pode ser restringido pela prevalência do direito à intimidade, e ser utilizado como desculpa e/ou forma de garantir a liberdade daqueles que praticam condutas ilícitas".[13]

Depreende-se do voto que o direito à privacidade foi relegado a uma posição inferior em relação ao direito à segurança e à proteção, sob o prisma da proporcionalidade, sem, contudo, adentrar em suas máximas, fazendo uma harmonização, considerando tão somente a maior ou menor relevância social. Para Fausto Santos de Morais[14], o mecanismo utilizado pelo julgador no caso acima não chegou nem a demonstrar a necessidade da interceptação, baseando-se somente pelos valores sociais, não levando em conta o disposto por Robert Alexy, que determina que o princípio previsto por lei formal deve ter um peso abstrato maior, devendo isso ser considerado no sopesamento.

11 SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. rev. e atual. Porto Alegre: Editora Livraria do Advogado, 2012. p. 403.

12 Art. 93, IX: "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade".

13 BRASIL. STF – *RHC nº 88371 SP*, Relator: Min. Gilmar Mendes, Data de Julgamento: 14/11/2006. Segunda Turma, Data de Publicação: DJ 02-02-2007.

14 MORAIS, Fausto Santos de. *Ponderação e Arbitrariedade*: A inadequada recepção de Alexy pelo STF. Salvador: Juspodvm, 2016. p. 130.

Por apresentar uma linha de raciocínio extremamente racional e argumentativa[15], o referido princípio proporciona a elaboração de uma decisão compatível com as exigências do dever de fundamentação judicial, que não sejam genéricas ou subjetivas e que possam permitir a ampla defesa, pois a complexidade do tema exige uma solução razoável e adequada.

3 Uma análise de direito comparado

A escolha pelo uso da análise do direito comparado justifica-se pela abrangência e relevância que o tema possui. A colisão de direitos fundamentais é algo muito delicado e que deve receber o tratamento adequado. Adentrar na realidade de um ordenamento estrangeiro e observar como este trata a matéria em foco mostra-se necessário. Uma comparação pode, muitas vezes, esclarecer dúvidas e apontar áreas para melhoramento. Os ordenamentos escolhidos demonstram divergências quanto às escolhas tomadas.

O primeiro a ser analisado é dos Estados Unidos da América, que notadamente busca a proteção da segurança pública nos mais elevados níveis, utilizando uma força massiva em prol da segurança pública. Busca-se entender se os mecanismos por ele adotados funcionam e no que consistem, realizando-se ao final alguns apontamentos quanto a uma possível ingerência de direitos fundamentais pela política de segurança adotada.

Posteriormente, parte-se para o estudo da jurisprudência do Tribunal Constitucional Alemão (*Bundesverfassungsgericht*) no que se relaciona ao conflito de preceitos constitucionais, como também dos dispositivos da Constituição Alemã (*Grundgesetz*) relacionados à matéria, tratando-se da dignidade humana e suas implicações no ordenamento jurídico. A análise se dá pela compreensão do quão preservados são os direitos fundamentais pela Carta Constitucional e quais são as restrições admitidas e por quais razões elas são admitidas, o que, na maioria das vezes, acontece pelo argumento da proteção à ordem e à segurança pública.

São colacionadas decisões elaboradas pela Corte Suprema da Alemanha, nas quais estão presentes elementos como a questão da violação da dignidade humana, da interceptação das comunicações e da violação de domicílios para a produção de provas na persecução penal. Após, é feita uma análise da Diretiva 24/2006 da União Europeia, a qual pode ser estudada em consonância com a Lei nº 9.296/96, posto que regulamenta

15 A "distinção entre âmbito de proteção e limites oferece significativas vantagens em termos de operacionalidade jurídico-temática, correspondendo à exigência de transparência metodológica, especialmente por não misturar interesses divergentes, além de implicar um ônus da justificação de uma restrição recaia sobre o intérprete que a invoca, o que apenas reforça a tese de que os fins não podem jamais justificar os meios, visto que não apenas o resultado, mas, sobretudo o caminho percorrido da conversão de uma posição *prima facie* (âmbito de proteção) em um direito (ou garantia) definitivo(a) afigura-se decisivo e viabiliza um controle de todo o procedimento". SARLET, Ingo Wolfgang. *Op.cit.* p. 399.

como se dará a intercepção dos tráfegos de dados na internet em prol da segurança pública. Observa-se, também, como a Corte Europeia considera os mecanismos de proteção previstos por referida diretiva com relação à violação da privacidade. A linha de exposição está sempre voltada à harmonização entre os preceitos fundamentais.

3.1 Estados Unidos da América e seus programas governamentais: uma possível ingerência de direitos fundamentais

A relação entre terrorismo e os Estados Unidos da América é estreita e ficou extremamente evidente após os ataques de 11 de Setembro, quando os prédios do *World Trade Center* foram destruídos por um ataque terrorista. A partir desse momento, o país todo se mobilizou no sentido de promover uma ação forte em resposta às forças terroristas, tendo como consequência a adoção de várias medidas de segurança máxima, como a intensiva fiscalização aérea e terrestre e a vigilância dos cidadãos.

A legislação criada às pressas é tipicamente de emergência, visando "proteger"[16] o país de um ataque iminente, mas sem o condão de estabelecer uma nova ordem legislativa sobre a matéria. O primeiro passo rumo à consolidação foi a edição do *Patriot Act* ou Lei Patriótica, aprovada em 26 de outubro de 2001, logo após aos fatídicos acontecimentos. Referido ato é o acrônimo de "***U**niting and **S**trengthening **A**merica by **P**roviding **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **A**ct*"[17], ou USA PATRIOT ACT, constituindo-se de 342 páginas que modificaram cerca de 15 leis federais existentes à época de sua promulgação.

O conteúdo trazido pelo ato é totalmente voltado à prevenção do terrorismo pela interceptação e violação de comunicações físicas ou digitais. Sua finalidade é "deter e punir atos terroristas nos Estados Unidos e ao redor do mundo, para melhorar a aplicação da lei de ferramentas investigatórias".[18] Pela seção 202, tem-se como permitida a ação da autoridade que intercepte uma comunicação via cabo, oral ou eletrônica, desde que relacionada a uma fraude computacional ou ofensas abusivas. Ainda, no Título II, observa-se que é permitida a divulgação do material coletado por um oficial a outro,

16 "É por essa dupla razão – proteger-nos dos perigos *e* de sermos classificados como um perigo – que temos investido numa densa rede de medidas de vigilância, seleção, segregação e exclusão. Todos nós devemos identificar os inimigos da segurança para *não sermos incluídos entre eles*. Precisamos acusar para sermos absolvidos, excluir para evitarmos a exclusão. Precisamos confiar na eficácia dos dispositivos de vigilância para termos o conforto de acreditar que nós, criaturas decentes que somos, escaparemos ilesos das emboscadas armadas por esses dispositivos – e que assim seremos reinvestidos e reconfirmados em nossa decência e na adequação de nossos métodos". BAUMAN, Zygmunt. *Op.cit*. p. 98.

17 "Unindo e Reforçando a America pela promoção de ferramentas necessárias à interceptação e obstrução do terrorismo". Tradução nossa.

18 ESTADOS UNIDOS DA AMÉRICA. *Patriot Act:* Public Law 107th-56 OCT 26, 2001- To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. 2001. Disponível em: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em: 24 mai. 2017.

inclusive das informações obtidas por meio de uma inteligência estrangeira que digam respeito à possibilidade de os Estados Unidos terem que dela se proteger.[19]

A regra interpretativa utilizada pela jurisprudência americana é a da demonstração de elementos probatórios mínimos que possam sustentar a acusação, conforme prevê a Quarta Emenda[20], a qual estabelece o direito de estar seguro e protegido contra buscas sem que haja uma causa provável e devidamente suportada. Contudo, posteriormente, o posicionamento foi se modificando com vistas à proteção do Estado ao invés do indivíduo, abrindo a possibilidade de afastar o suporte probatório mínimo acima apontado quando esteja em jogo a defesa nacional. O exigido passou a ser apenas a concretude do objeto e a duração da investigação. Ou seja, a exigência existe, bem como sua exceção, tornando incerta a aplicação da lei.

Quando a interceptação ocorria sem a autorização, por qualquer motivo, exigia-se que fosse minimamente razoável e condizente entre meios e fins[21]. Portanto, sentindo-se a necessidade de investigar um cidadão que possa estar prestes a cometer um ato terrorista e não havendo tempo para a obtenção de uma autorização, a investigação deve se dar de maneira cautelosa, não indo além do necessário à coleta das informações. Em 1978, foi instituída uma Corte responsável por analisar os pedidos de interceptação feitos pelas autoridades americanas, como a Agência de Segurança Nacional (NSA) e o FBI. Essa corte recebeu o nome de FISA[22] (*Foreign Intelligence Surveillance Court*), ou Tribunal de Vigilância de Inteligência Estrangeira, e tem o poder de permitir a interceptação de comunicações estrangeiras sem um mandado judicial[23].

Cabe informar que, desde sua criação até o início de setembro de 2001, o número de utilização da corte foi de 47 vezes, e de setembro de 2001 até o final de 2002, 113 vezes[24]. Ou seja, tem-se um Tribunal de exceção, fundamentado exclusivamente na

19 Ibidem.

20 A Quarta Emenda assim prescreve: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". ESTADOS UNIDOS DA AMÉRICA. *Constitution of the United States*. 1787. Disponível em: < https://www.senate.gov/civics/constitution_item/constitution.htm>. Acesso em: 24 maio 2017.

21 Conforme o Título III do *Omnibus Crime Control and Safe Secret Act*, de 1968.

22 Ver <http://www.fisc.uscourts.gov/>.

23 Conforme diz Julian Assange na obra *Quando o Google encontrou o Wikileaks,* "Em 2003, a Agência de Segurança nacional (NSA, na sigla em inglês) já violava sistematicamente a Lei de Vigilância de Inteligência Estrangeira (Fisa, em inglês), sob a direção do general Michael Hayden. Isso foi na época do programa Total Information Awareness [Conhecimento de Informação Total]. Antes que se sonhasse com o Prism, por ordem da Casa Branca de Bush a NSA já tinha o objetivo de 'coletar tudo, farejar tudo, processar tudo, explorar tudo'". ASSANGE, Julian. *Quando o Google encontrou o Wikileaks*. Trad. Cristina Yamagami. 1. ed. São Paulo: Boitempo, 2015. p. 38.

24 LICHTBLAU, Eric. *Justice Dept. Lists Use of New Power to Fight Terror.* The New York Times, 2003. Disponível em: < http://www.nytimes.com/2003/05/21/politics/21PATR.html>. Acesso em: 24 mai. 2017.

permissão de interceptações sem a necessidade de se recorrer ao Judiciário, causando insegurança jurídica. Surgem, então, dois problemas, quais sejam o da impossibilidade de fiscalização e conhecimento das decisões dadas pela FISA e a profundidade das investigações realizadas pelas autoridades americanas, que podem ir bem além do razoável. As investigações podem ir muito além do objeto informado à Corte, causando extrema incerteza quanto a sua legitimidade.

O FBI, agência de investigação americana, possui um sistema próprio de monitoramento de dados na internet. Primeiramente, o software utilizado era o *Carnivore*, implantado em 1997, que era considerado um tanto quanto simplificado e ultrapassado, sendo substituído em 2005 pelo *NarusInsight,* de natureza mais complexa e capaz de um processamento de dados em larga escala e em alta velocidade, mais confiável na análise e captação de informações. Recentemente houve um escândalo de espionagem ocorrido no Brasil e promovido pela NSA, a qual possivelmente estaria vigiando o que os usuários brasileiros fazem na internet.

> Para facilitar sua ação global, a NSA mantém ainda parcerias com as maiores empresas de internet americanas. [...] o software Prism permite à NSA acesso a e-mails, conversas on-line e chamadas de voz de clientes de empresas como Facebook, Google, Microsoft e YouTube.[25]

O PRISM, programa de espionagem acima citado, é mantido pela Agência Nacional de Segurança dos Estados Unidos (NSA), e visa à vigilância e à guarda de dados na Internet com a finalidade de proteger o país de possíveis ameaças à segurança pública (terrorismo). O programa foi iniciado em 2001, sendo alegada a necessidade de adaptação ao mundo digital e à vida na internet. Para tanto, a agência americana fez parcerias com as maiores empresas do ramo das comunicações na internet, as quais passaram a dar suporte às ações do governo, promovendo o cumprimento de ordens judiciais e criando *backdoors*[26] em seus bancos de dados, dando total acesso aos dados das comunicações à NSA.

Nas palavras da agência americana, "técnicos da NSA instalaram estações interceptoras em pontos de junção chave, ou interruptores, por todo o país"[27]. Esses

25 O GLOBO. *Relembre o caso de espionagem da NSA a cidadãos e empresas no Brasil.* 2013. Disponível em: <http://oglobo.globo.com/pais/relembre-caso-de-espionagem-da-nsa-cidadaos-empresas-no-brasil-9782018> Acesso em: 24 mai. 2017.

26 *Backdoor* é uma ferramenta que possibilita o controle e o acesso às informações de um servidor remoto. No caso em tela, do local onde ficam armazenados os dados das empresas de comunicações.

27 No original: "NSA technicians have installed intercept stations at key junction points, or switches, throughout the country". ESTADOS UNIDOS DA AMÉRICA. National Security Agency. Domestic Surveillance Directorate. *Surveillance Techniques*: How Your Data Becomes Our Data. Disponível em: <https://nsa.gov1.info/surveillance/>. Acesso em: 24 mai. 2017.

interruptores estão localizados nas maiores empresas de telecomunicações do mundo, controlando o tráfego e o fluxo da internet nos Estados Unidos. Dentre as principais empresas, estão a Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, e Apple. Segundo a agência, essa parceria permite acesso direto a "áudio, vídeo, fotos, e-mails, documentos e dados de conexão de cada um dos sistemas"[28]. Ainda, há casos protagonizados pela Agência Brasileira de Segurança (ABIN). Motivado pela recente onda de manifestações que ocorreram no Brasil, o Governo, para prevê-las, teria decidido monitorar o WhatsApp.

> [...] a Agência Brasileira de Inteligência (Abin) montou às pressas uma operação para monitorar a internet. O governo destacou oficiais de inteligência para acompanhar, por meio do Facebook, Twitter, Instagram e WhatsApp, a movimentação dos manifestantes. [29]

Dentro dessa temática, é necessário falar do tratado de assistência legal mútua em matéria criminal celebrado entre o Brasil e os Estados Unidos em 1997, promulgado pelo Decreto nº 3.810/2001. Conforme consta do acordo[30], no desejo de melhorar a aplicação da lei pelas autoridades de ambos os países na investigação, acusação, e prevenção de crimes por meio da mútua cooperação legal e assistência em matéria criminal, foi assinado o tratado.

Referido documento prevê que a assistência deve tomar depoimento de pessoas; providenciar documentos ou gravações; localizar e identificar pessoas ou coisas; executar requisições de buscas ou qualquer outra assistência não proibida pela lei dos países. São previstas ainda outras especificações como a impossibilidade de investigação se o crime estiver previsto na legislação militar. Ainda, existe um tópico que trata dos requisitos do pedido, quais sejam, o nome da autoridade que conduz a investigação; a descrição da matéria e a natureza da investigação; descrição da prova ou da assistência pretendida; declaração de qual a finalidade da prova.

Tais exigências caracterizam o mínimo necessário para a realização da diligência e preveem a obrigatoriedade de informar a natureza da investigação, a descrição e a finalidade da prova. Do exposto, pode-se perceber que uma nação, quando movida pelo medo, pode criar os mais diversos mecanismos para proteger-se. Os Estados Unidos, após serem atacados, rapidamente iniciaram uma revolução no modo como lidavam

28 No original: "audio, video, photographs, e-mails, documents and connection logs for each of these systems". Ibidem.

29 MONTEIRO, Tania; RIZZO, Alana. *Abin monta rede para monitorar a internet***.** 2013. Disponível em: <http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm>. Acesso em: 24 mai. 2017.

30 Ver <http://www.state.gov/documents/organization/106962.pdf>.

com ameaças terroristas. Uma enxurrada de inovações legislativas tomou lugar e começou a determinar os passos do país na luta pela segurança.

Muitas dessas inovações, por um lado, podem dar uma maior sensação de proteção aos cidadãos e à nação, mas por outro, podem ser consideradas como uma grande afronta aos direitos individuais, tão duramente conquistados, e inclusive, garantidos constitucionalmente pela Constituição Americana. Assim, restam a reflexão e o sopesamento de ideais, culminando na questão da possibilidade de se abrir mão de muitas garantias em prol da luta contra o terrorismo.

3.2 A Constituição (*Grundgesetz*) e a jurisprudência do Tribunal Constitucional Alemão (*Bundesverfassungsgericht*) no que diz respeito à colisão de direitos fundamentais

Essa parte será dedicada à compreensão da Constituição da República Federativa da Alemanha e da produção jurisprudencial do Tribunal Constitucional Alemão voltada para a colisão de direitos fundamentais. Buscar-se-á analisar a linha de pensamento, raciocínio e argumentação utilizada pela Corte como forma de elucidar alguns pontos desse trabalho.

A Constituição Alemã (*Grundgesetz*), logo em seu primeiro artigo, emana que "A dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público"[31], passando a ideia de que a dignidade humana é intocável, absoluta e irredutível. Porém, a interpretação dada não deve ser essa.

Entende-se que a dignidade funcionaria não como norma absoluta, mas de observância obrigatória, pois dela decorrem vários direitos, podendo sempre ser atingida por via colateral ou indireta. Em uma decisão do ano de 1970 (*BVerfGE* 30, 1), a Corte Alemã optou por declarar a Constitucionalidade, via controle abstrato, de uma emenda Constitucional que visava limitar o sigilo de correspondência, postal e de telecomunicação, sob a argumentação de não haver violação à dignidade humana. Assim,

> No que diz respeito ao princípio da inviolabilidade da dignidade humana, firmado no Art. 1 GG, o qual, segundo o Art. 79 III GG, não pode ser atingido por emenda constitucional, tudo depende de se determinar que condições devem estar presentes para que a dignidade humana possa ser considerada como violada. Evidentemente não se pode falar em termos gerais, mas sempre em face do caso concreto. [...] O tratamento da pessoa humana pelo poder público que cumpre a lei deve, para se verificar se a dignidade humana foi atingida, ser expressão do desrespeito ao valor a

31 ALEMANHA. *Lei Fundamental da República Federal da Alemanha*. 1949. Trad: Assis Mendonça. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso em: 24 mai. 2017.

> que o ser humano tem direito por força de sua existência como pessoa, configurando, portanto, nesse sentido, 'um tratamento desrespeitoso'.[32]

Do colocado pelo Tribunal, pode-se entender que nem sempre a dignidade humana terá um caráter intangível como demonstra a Constituição Alemã. Depende-se sempre, como assevera o excerto acima, de como as relações se deram no caso concreto, pois este é que irá determinar em que pontos houve ou não a violação de um direito. A verificação para aferir se a dignidade humana foi atingida depende da variante "houve desrespeito ao valor do ser humano como pessoa por implicação de sua existência como pessoa?".

Dentro da problemática envolvendo a limitação da dignidade humana, passa-se a elucidar como se dá o tratamento pelo ordenamento alemão quanto à inviolabilidade das comunicações e do domicílio. Conforme estabelece o artigo 10 da Constituição Alemã, "O sigilo da correspondência, assim como das comunicações postais e da telecomunicação é inviolável", sendo que "limitações só podem ser ordenadas em virtude de lei". Se a limitação tiver por finalidade a proteção da ordem democrática ou a existência e segurança da Federação, "a lei pode determinar que a limitação não seja levada ao conhecimento do indivíduo atingido"[33].

Pelo contido no artigo 13, o domicílio é inviolável, sendo que buscas só poderão ser ordenadas por um juiz, e caso a demora constitua perigo. Ainda, quando houverem fundadas suspeitas de que o delito cometido é grave, "poderão ser utilizados, com base numa autorização judicial, recursos técnicos de vigilância acústica das residências nas quais se encontra presumivelmente o suspeito", com a condição de que por outra forma, a investigação dos fatos se torne desproporcionalmente difícil ou sem perspectiva de êxito, devendo ainda a medida ter duração limitada. Referido artigo é encerrado da seguinte maneira,

> […] só podem ser praticadas intervenções ou restrições que afetem esta inviolabilidade na defesa contra perigo comum ou perigo de vida individual; em virtude de lei, tais medidas também podem ser praticadas *com o fim de prevenir perigos iminentes para a segurança e a ordem públicas*.[34]

Pelo contido no artigo acima transcrito, nota-se que o legislador buscou proteger o domicílio, declarando-o inviolável, mas, ao mesmo tempo, previu as exceções que

32 SCHWABE, Jürgen. *Cinquenta anos de jurisprudência do Tribunal Constitucional Alemão.* Org. MARTINS, Leonardo. Trad. HENNIG, Beatriz. et al. Montevideo: KONRAD-ADENAUER-STIFTUNG E. V., 2005. p. 180-181.

33 ALEMANHA, *Op.cit.* s.p.

34 Ibidem. Grifo nosso.

comportam o significado de inviolável. Assim, quando houver perigo da demora da diligência, não havendo possibilidade de se esperar pela produção da prova, a busca poderá ser autorizada.

Ainda, se houver fortes indícios da extrema gravidade do delito, está permitida a utilização de recursos de vigilância sonora em que se encontra o possível agente. Porém, tal disposição atrela-se a outra regra, que é a da possibilidade de a investigação resultar prejudicada ou sem esperança de sucesso. Ao final, tem-se a disposição que limita a incidência das interceptações para as situações que possam resultar em perigo de vida, comum ou individual, sendo que as ações podem ter o fim de *prevenir* perigos à *ordem* e à *segurança pública*. A jurisprudência abaixo (*BVerfGE* 109, 279) exemplifica bem o tema,

> A vigilância acústica de dependências domiciliares para fins de persecução penal não viola, em geral, o conteúdo de dignidade humana do Art. 13 I GG e Art. 2 I c.c. Art. 1 I GG. Porém, podem, o tipo e o modo da realização da vigilância acústica domiciliar, levar a uma situação na qual a dignidade humana restará violada. Para que isso seja evitado, o Art. 13 III GG especifica expressamente providências jurídicas a serem tomadas; somam-se a elas outros pré-requisitos construídos por interpretação constitucional. A autorização constitucional para a introdução da vigilância acústica domiciliar, contida no Art. 13 III GG, não fere, por isso, o Art. 79 III GG, pois a indispensável regulamentação legal pode e precisa garantir que a dignidade humana, no caso concreto, não será violada. [...] As normas do código de processo penal para a realização da vigilância acústica do domicílio para fins de persecução penal não satisfazem totalmente as exigências constitucionais em relação à proteção da dignidade humana (Art. 1 I GG), o princípio da proporcionalidade abrangido pelo princípio do Estado de direito, a garantia de efetiva proteção jurídica (Art. 19 IV GG) e o direito à ampla defesa e ao contraditório (Art. 103 I GG). [35]

Depreende-se, portanto, que as interceptações acústicas em domicílios não acarretam, necessariamente, uma violação ao conteúdo da dignidade humana. Existirão certas situações em que a ostensividade dos meios usados ou o abuso da investigação acarretam na violação do princípio acima descrito. Todavia, se houver uma utilização comedida, dentro das previsões legais, que respeite o imprescindível a persecução penal, não será vislumbrada afronta ao seu conteúdo.

A decisão continua prescrevendo que as normas do Código de Processo Penal não atendem às exigências constitucionais impostas pelo Constituinte no que tange a proteção da dignidade humana, bem como à ampla defesa e ao princípio da

35 SCHWABE, Jürgen. *Op.cit*. p. 692-695.

proporcionalidade. Restando assim, ao aplicador da lei, durante a formulação de sua decisão, usar toda a técnica e argumentação jurídica possível, pondo em prática o princípio acima citado, sob pena de ofender a Constituição.

É possível constatar que tanto a legislação quanto a jurisprudência alemã se mostram cientes da possibilidade de ocorrência de uma colisão de direitos fundamentais, prevendo, para tanto, normas claras e precisas, que orientam aquele que as aplicará. A construção jurisprudencial acompanha a legislativa, procurando-se sempre harmonizar-se, culminando num sistema que funciona muito próximo do ideal.

3.3 A Diretiva 24/2006 da União Europeia

Será aqui feita uma análise de como o ordenamento europeu trata a relação entre privacidade e segurança pública. Estuda-se a diretiva 24/2006 da União Europeia e a Lei nº 32/2008 da República Portuguesa, que é uma ramificação da referida diretiva. No ano de 2006, a União Europeia decidiu por instituir a diretiva de número 24, a qual traz questões relativas à conservação de dados gerados ou tratados no contexto da prestação de serviços públicos de comunicações eletrônicas acessíveis ou de redes públicas de comunicações.

No artigo primeiro, está seu objeto, que é regular a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registrado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes[36]. Com previsão expressa em seu artigo 15, a diretiva impõe que seja feita uma regulamentação legislativa pelos estados membros da União Europeia. Por conseguinte, Portugal foi um dos países que efetivou tais disposições pela Lei nº 32/2008, a qual, por meio de seu texto, regulamenta a questão da guarda de dados da internet.

Em referida lei, pode-se perceber claramente a possibilidade de invasão de privacidade para a repressão de crimes, conforme disposto no artigo 3º "A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes"[37]. Mais adiante, no artigo 9º, dispõe-se que a transmissão dos dados referentes às interceptações só poderá

36 UNIÃO EUROPEIA, *Diretiva 24/2006, de 13 de abril de 2006.* Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva nº 2002/58/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32006L0024>. Acesso em: 24 mai. 2017.

37 PORTUGAL. *Lei n. 32/2008, de 17 de julho de 2008.* Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. Disponível em: <http://www.dre.pt/pdfgratis/2008/07/13700.pdf>. Acesso em: 24 mai. 2017.

ser permitida por despacho fundamentado do juiz se houver razões para crer que a diligência é indispensável à descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

Ainda em seu artigo nono, encontra-se uma previsão de suma importância, qual seja a de que "a decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade"[38]. Deveras, notável tal disposição que prescreve a observância do uso do princípio da proporcionalidade. E de outro modo não poderia ser, pois se objetiva a harmonização de direitos fundamentais, o melhor modo de se fazer isso é analisar o caso concreto sob a influência das máximas da adequação e necessidade, bem como do sopesamento dos interesses, pela proporcionalidade em sentido estrito.

Em recente decisão proferida pela Corte de Justiça da União Europeia, declarou-se inválida a retenção de dados da internet, invalidando, consequentemente, a diretiva 24/2006. O fundamento trazido pela corte é o de que, ao exigir a retenção desses dados e permitir que as autoridades nacionais competentes os acessem, a diretiva interfere de uma forma particularmente grave com os direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais.

Ainda, para a corte, ao adotar a diretiva relativa à conservação de dados, a União Europeia ultrapassou os limites impostos pela observância do princípio da proporcionalidade. A ampla e particularmente grave interferência da diretiva com os direitos fundamentais em causa não é suficientemente circunscrita para garantir que a interferência seja realmente limitar-se ao estritamente necessário. Desse modo,

> No que respeita ao caráter necessário da conservação dos dados imposta pela Diretiva 2006/24, cabe observar que é verdade que a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, assume primordial importância para garantir a segurança pública e a sua eficácia pode depender em larga medida da utilização das técnicas modernas de investigação. No entanto, tal objetivo de interesse geral, por mais 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. Quanto ao direito ao respeito pela vida privada, em conformidade com jurisprudência constante do Tribunal de Justiça, a proteção deste direito fundamental exige, em quaisquer circunstâncias, que as derrogações à proteção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário.[39]

38 Ibidem.

39 LUXEMBURGO. Corte de Justiça da União Europeia. *Acórdão de C-293/12 e C-594/12 Direitos Digitais Irlanda, Seitlinger e Outros*. 2014.

Percebe-se, da fundamentação dada pela corte, que a Diretiva 24/2006 da União Europeia não respeitava os limites do direito à privacidade, extrapolando o que é considerado razoável, sendo, desse modo, declarada inválida. Observou-se que, nesse caso, a privacidade tomou um caráter protagonista, devendo ser respeitada, em que pese a apuração de crimes.

5 Considerações Finais

Durante o trabalho, procurou-se mostrar as implicações que a vigilância digital presente na modernidade pode ter no Direito, principalmente quanto à preservação da privacidade em meios eletrônicos. A partir do paradoxo apresentado entre a garantia da segurança pública e a privacidade, entendeu-se a existência de um conflito entre direitos fundamentais, sendo necessário então buscar uma resposta para a solução do conflito.

No que se refere à investigação e à prevenção de crimes, o regramento pátrio é dado pela Lei nº 9.296/96, a qual possibilita o uso de interceptações informáticas (dados digitais), desde que por decisão judicial devidamente fundamentada. A fim de resolver o problema proposto, buscaram-se respostas no princípio da proporcionalidade, tendo em vista a inexistência de direitos absolutos e a importância de efetividade dos direitos fundamentais.

O objetivo do trabalho foi analisar como ordenamentos jurídicos estrangeiros tratavam a matéria, retratando como era procedida a vigilância digital e a interceptação de dados pelos governos e se a proporcionalidade era prevista pela legislação e utilizada pelos tribunais. Observou-se que, nos Estados Unidos da América, a luta contra o terrorismo prevalece sobre a preservação da privacidade, sendo que os instrumentos de vigilância e de prevenção de crimes são extremamente poderosos.

Na Alemanha, percebeu-se que os direitos fundamentais de proteção ao domicílio e de preservação à vida privada são invioláveis, contudo, o próprio texto constitucional já determina as possíveis exceções a tal inviolabilidade, não abrindo margem para criação judiciária, a qual fica encarregada de julgar, baseando-se no caso concreto. Observou-se que na União Europeia, mesmo existindo legislação específica determinando a invasão da privacidade em prol da segurança pública, os Tribunais Constitucionais têm entendido que tais determinações são inválidas, incorrendo em flagrante desrespeito ao direito à privacidade.

Destarte, a análise do tratamento dispensado ao tema mostrou que alguns países dão uma maior promoção à preservação da privacidade do que outros, que, em nome da garantia da segurança pública, acabam por aplicar uma intensiva fiscalização nas trocas de dados digitais. A observância da proporcionalidade se mostrou presente, embora os Estados Unidos não a utilizaram. Assim, conclui-se que a utilização da proporcionalidade é extremamente importante, devendo as medidas que procederem ou autorizarem as interceptações informáticas observá-la.

Referências

ALEMANHA. *Lei Fundamental da República Federal da Alemanha*. 1949. Trad: Assis Mendonça. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso em: 24 mai. 2017.

ALEXY, Robert. *Teoria dos direitos fundamentais*. 2. ed. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2012.

ASSANGE, Julian. *Quando o Google encontrou o Wikileaks*. Trad. Cristina Yamagami. 1. ed. São Paulo: Boitempo, 2015.

BAUMAN, Zygmunt. *Modernidade Líquida*. Trad. Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001.

_____. *Comunidade*: a busca por segurança no mundo atual. Trad. Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2003.

_____. *Vigilância Líquida*: diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BRASIL. STF. *RHC nº 88371 SP*, Relator: Min. Gilmar Mendes, Data de Julgamento: 14/11/2006. Segunda Turma, Data de Publicação: DJ 02-02-2007.

CAVALIERI FILHO, Sérgio. *Programa de Sociologia Jurídica*. Rio de Janeiro: Forense, 2007.

DA SILVA, Eliezer Gomes; GIACOIA, Gilberto. Provas lícitas não repetíveis, autorizadas por decisões com deficiência de fundamentação: nulidade e inadmissibilidade da prova, nas interceptações telefônicas, e o necessário emprego da técnica de ponderação. In: Anais *do XXIV Congresso Nacional do CONPEDI - UFMG/FUMEC /Dom Helder Câmara – Processo Penal e Constituição*. Florianópolis: CONPEDI, 2015.

ESTADOS UNIDOS DA AMÉRICA. *Constitution of the United States*. 1787. Disponível em: <https://www.senate.gov/civics/constitution_item/constitution.htm>. Acesso em: 24 mai. 2017.

_____. *Patriot Act*: Public Law 107th-56 OCT 26, 2001- To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. 2001. Disponível em: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em: 24 mai. 2017.

_____. National Security Agency. *Domestic Surveillance Directorate. Surveillance Techniques*: How Your Data Becomes Our Data. Disponível em: <https://nsa.gov1.info/surveillance/>. Acesso em: 24 mai. 2017.

LICHTBLAU, Eric. Justice Dept. *Lists Use of New Power to Fight Terror*. The New York Times, 2003. Disponível em: <http://www.nytimes.com/2003/05/21/politics/21PATR.html>. Acesso em: 24 mai. 2017.

LUXEMBURGO. Corte de Justiça da União Europeia. *Acórdão de C-293/12 e C-594/12 Direitos Digitais Irlanda, Seitlinger e Outros*. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=120934>. Acesso em: 24 mai. 2017.

MONTEIRO, Tania; RIZZO, Alana. *Abin monta rede para monitorar a internet*. 2013. Disponível em: <http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm>. Acesso em: 24 mai. 2017.

MORAIS, Fausto Santos de. *Ponderação e Arbitrariedade*: A inadequada recepção de Alexy pelo STF. Salvador: Juspodvm, 2016.

MORAIS, Fausto Santos de; ZOLET, Lucas. Constitutional rights expansion and contributions from Robert Alexy's theory / A expansão dos direitos fundamentais e a contribuição teórica de Robert Alexy. *Revista Brasileira de Direito*, Passo Fundo, v. 12, n. 2, p. 127-136, dez. 2016. ISSN 2238-0604. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/1505/1006>. Acesso em: 24 mai. 2017. doi: http://dx.doi.org/10.18256/2238-0604/revistadedireito.v12n2p127-136

O GLOBO. *Relembre o caso de espionagem da NSA a cidadãos e empresas no Brasil*. 2013. Disponível em: <http://oglobo.globo.com/pais/relembre-caso-de-espionagem-da-nsa-cidadaos--empresas-no-brasil-9782018>. Acesso em: 24 mai. 2017.

PINHEIRO, Patricia Peck. *Direito Digital*. 5. ed. rev. atual. ampl. São Paulo: Saraiva, 2013.

PORTUGAL. *Lei n. 32/2008, de 17 de julho de 2008*. Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. Disponível em: <http://www.dre.pt/pdfgratis/2008/07/13700.pdf>. Acesso em: 24 mai. 2017.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 11. ed. rev. e atual. Porto Alegre: Editora Livraria do Advogado, 2012.

SCHWABE, Jürgen. *Cinquenta anos de jurisprudência do Tribunal Constitucional Alemão*. Org. MARTINS, Leonardo. Trad. HENNIG, Beatriz. et al. Montevideo: KONRAD-ADENAUER-STIFTUNG E. V., 2005.

UNIÃO EUROPEIA. *Diretiva 24/2006, de 13 de abril de 2006*. Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva nº 2002/58/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32006L0024>. Acesso em: 24 mai. 2017.