A TÉCNICA INFORMACIONAL COMO FERRAMENTA DE REDUÇÃO DA PRIVACIDADE NA REDE: ANÁLISE DO CASO WIKILEAKS

THE INFORMATIONAL TECHNIQUE AS A TOOL TO REDUCE PRIVACY ON THE WEB: ANALYSIS OF THE WIKILEAKS CASE

Patrícia Borba Marchetto[1]
Jorge David Barrientos-Parra[2]
Gustavo Alarcon Rodrigues[3*]

RESUMO

O presente artigo tem como foco analisar os impactos causados pelas tecnologias computacionais e informacionais, em especial a internet e suas ferramentas acessórias, sobre a privacidade humana, direcionando a abordagem para a atuação dos Estados e grandes corporações do ramo digital, estes expostos nas denúncias produzidas pelo *site* "*Wikileaks"*. Parte-se, portanto, de uma análise da técnica computacional, sua velocidade de expansão e suas bases fundantes, visando compreender as dinâmicas de poder que se engendram através da internet e as suas diferenças quando comparadas com o poder exercido no "domínio dos átomos", para assim encaminhar à abordagem das manifestações de poder enquanto violações à privacidade voltadas à estruturação de meios de controle e vigilância. O trabalho em questão tem como paradigma metodológico, em um primeiro momento, o método dedutivo, partindo de concepções teóricas gerais para compreender a dinâmica de forças na internet e, durante a abordagem da situação prática, o método indutivo, demonstrando por meio do caso paradigmático como tais forças atuam sob o manto da alegalidade, propondo concepções convergentes com as sínteses obtidas dedutivamente. Importante ressaltar que há a adoção da revisão bibliográfica de obras, artigos e notícias relacionadas ao tema como suporte à metodologia optada.

[1] Doutora em Direito pela Universitat de Barcelona, Espanha. Professora vinculada ao Programa de Pós-graduação em Direito da Faculdade de Ciências Humanas e Sociais, da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). Professora Assistente Doutora do Departamento de Administração Pública da Faculdade de Ciências e Letras de Araraquara-SP, da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP).

[2]Doutor em Direito pela Université Caholique de Louvain(UCL), Bélgica. Professora vinculada ao Programa de Pós-graduação em Direito da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP).
Professor Assistente Doutor do Departamento de Administração Pública da Faculdade de Ciências e Letras de Araraquara-SP, da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP).

[3] Mestrando do Programa de Pós-graduação em Direito da Universidade Estadual Paulista "Júlio de Mesquita Filho". Bacharel em Direito pela Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista "Júlio de Mesquita Filho". Advogado.

Palavras-chave: internet. Wikileaks. privacidade. vigilância.

ABSTRACT

The present work aims to analyze impacts caused by computer and information technologies, on human privacy, especially the internet and its accessory tools, directing the approach to State and large digital corporations' behavior, these exposed by Wikileaks website. Therefore, it starts from an analysis of computational technique, its speed of expansion and its founding bases, aiming to understand the dynamics of power that are generated through the internet and their differences when compared to the power exercised in the "domain of atoms". Through this, is sought to address the exposing form of power as privacy violations, connected to structuring means of control and surveillance. The work in question has as a methodological paradigm, at first, the deductive method, starting from general theoretical conceptions to understand the dynamics of forces on the internet. During the approach of the practical situation, the inductive method is used, demonstrating through the paradigmatic case how these forces operate under the cover of legality, proposing concepts that converge with the syntheses obtained deductively. It is important to note that there is the adoption of a bibliographic review of works, articles and news related to the theme as support for the chosen methodology.

Keywords: internet. Wikileaks. privacy. surveillance.

1. INTRODUÇÃO

Os avanços da computação e a dinamização dos fluxos de informação, em especial com o desenvolvimento da internet, trouxeram uma gama de discussões orientadas para a compreensão dos prováveis riscos que acompanhariam de perto os benefícios que eram trazidos em um ritmo cada vez maior por essas novas tecnologias. Sem dúvida, na primeira metade do século XX, ainda sem conhecer a revolução digital, George Orwell já apresentava em sua obra célebre "1984" uma visão pessimista dos incrementos causados nos meios de circulação de informações e na técnica eletroeletrônica, exibindo modelos, até então distópicos, de realidade no qual a humanidade e suas bases de liberdade e privacidade se viam totalmente inviabilizadas pelo aparelhamento técnico do Estado e dos meios de controle. Ainda pautado na ficção, o autor apresentava uma visão geral acerca do incremento técnico e sua utilidade para fins de dominação. Essa abordagem pessimista opunha-se totalmente ao modelo eufórico e entusiasta de recepção das novas técnicas pela sociedade, modelo este muito bem expresso na visão de Isaac Asimov acerca dos direcionamentos da robótica e da técnica avançada.

A visão de Orwell, até então tida como ficcional, passa a tomar contornos de realidade quando a técnica computacional e informacional adquiriram relevância socioeconômica e política, havendo a expansão dos meios computacionais e do acesso à internet. A ampliação do ambiente virtual, por meio do maior acesso às redes e incremento dos aparelhos computacionais, passa a permitir que haja a sua utilização enquanto ferramenta do poder, seja ele econômico ou político, garantindo a existência de mecanismos de vigilância e controle exercidos por detrás do aspecto neutro e isento da internet. A privacidade, diante da expansão dos mecanismos de dominação, sofre reiteradas lesões, sendo estas marcadas pela invisibilidade dos mecanismos e pela reiteração das práticas por parte dos Estados e corporações.

Assim, tomando como paradigma os casos expostos no site "*Wikileaks"*, especificamente os relatórios *Spy Files e Vault 7*, é necessário aprofundar a pesquisa sobre as dimensões do exercício do poder por meio da internet, assimilando as decorrências diretas da técnica e seu papel no constructo de vigilância, visando compreender as dificuldades ou mesmo impossibilidades de manifestação jurídica do poder por meio dos ambientes virtuais, diretamente vinculadas às atuação ilegais perpetuadas pelos agentes estatais e econômicos, para assim, diante dessa contextualização, compreender como ocorrem as violações sobre a privacidade humana dentro do ambiente virtual e visualizar os impactos causados pelo caso *"Wikileaks"*.

2. A INTERNET E A TÉCNICA COMPUTACIONAL

O desenvolvimento de aparelhos computacionais, que data da metade do século passado, recebeu um expressivo empuxo quando foram desenvolvidos mecanismos eficazes de intercomunicação entre esses aparelhos, estabelecendo uma rede de sistemas computacionais capazes de circular informações e, dessa forma, estruturar todo um ambiente virtual capaz de reproduzir a vivência humana. Paul Armer, ainda no ano de 1975 (ARMER, 1975, p.3), já afirmava que a velocidade dos circuitos computacionais aumentava em uma ordem de magnitude de dez vezes[4] em aproximadamente quatro ou cinco anos, enquanto as demais áreas da indústria, não correlacionadas ao âmbito computacional, cresciam em uma ordem de magnitude semelhante em aproximadamente um século. Assim, ainda na primeira

[4] Sob uma ordem de magnitude de 10 vezes, quer ser dito que a cada período de tempo há um aumento de cerca de 10 vezes no poder de processamento de dados.

década de vida da internet, a velocidade de expansão das capacidades de processamento atingia a amplitude de a cada quatro anos ser cerca de dez vezes maior que o poder de processamento nos anos anteriores, alcançando dessa forma uma ordem de magnitude cada vez maior até atingir, condição esta que foi capaz de estabelecer redes cada vez mais potentes, com a possibilidade de circular informações cada vez mais complexas em um tempo cada vez menor.

Paul Armer, ex-diretor do Centro de computação da Universidade de Standford (ARMER, 1975, 4), já apontava que a indústria da tecnologia computacional dava passos rumo a uma expansão múltipla, incluindo mecanismos de processamento digital em quase todos os bens de consumo, como carros, caminhões, e "tudo aquilo que comportasse uma engrenagem", como decorrência direta da redução dos preços desses chips de processamento. Como consequência disso, haveria o barateamento a ponto dos meios computacionais (*hardwares*) tornarem-se quase gratuitos, contrapondo-se a um crescimento exponencial dos custos de programação computacional e de circulação informacional, migrando o foco geral da técnica do desenvolvimento computacional para a programação, circulação e gerenciamento de informações, compondo a chamada técnica informacional avançada.

Decorrendo diretamente da capacidade crescente de processamento informacional e do desenvolvimento de meios ágeis de difusão, há o aperfeiçoamento dos meios de comunicação digital, especificamente a chamada internet. Scott Feir (FEIR, 1997, p.362-363) apresenta, de forma técnica, a internet como um grupo de computadores interligados que se comunicam por meio de protocolos TCP/IP, conectados por meios de redes telefônicas de velocidade para compartilhar informações[5]. Desde o desenvolvimento da ARPANet pelo Departamento de Defesa dos Estados Unidos da América no ano de 1969, modelo que promoveu a primeira interligação entre bases militares de pesquisa e padronizou os protocolos de comunicação digital, houve uma expansão do ambiente digital em mais de vinte e três vezes seu tamanho, até a data de 1996 (ZAKON, 1996), chegando hoje a circular anualmente mais de 2 zetabytes de informação (2×10^{21} bytes).

Atualmente, vivemos em um mundo conectado, marcado pelo abuso dos meios virtuais, com a utilização diuturna de *smartphones*, computadores, dispositivos vestíveis, automação doméstica, veículos conectados à rede ou mesmo automatizados, digitalização de sistemas públicos de serviços, virtualização de sistemas governamentais, públicos ou secretos, automação de estruturas produtivas, todas essas estruturas e mecanismos ligados diretamente

[5] "The internet is a group of computer networks that communicate using TCP/IP protocol, and are connected though speed telephone lines for the purpose of sharing information" (FEIR, 1997, p.362-363).

à rede mundial de computadores. Assim como previu Paul Armer, houve o barateamento das técnicas de produção de *hardwares* de processamento, com a expansão dessa capacidade para grande parte dos bens de consumo, tornando-os aptos para engendrarem comunicações com a rede mundial de computadores, estabelecendo a chamada dinâmica da internet das coisas.

No entanto, a estruturação massiva da rede mundial de computadores e a entrada de um número cada vez maior de usuários causou certa dificuldade de gestão, que refletiu numa clara crise do direito sobre o âmbito virtual. O surgimento da internet não se mostra como o fenômeno de maior importância quando analisado o histórico do ambiente virtual de circulação de informações, sendo dada a maior importância à expansão massiva dos domínios da rede e a popularização atrelada ao seu acesso, permitindo que uma rede, antes vinculada a órgãos governamentais de pesquisas e grandes corporações, pudesse ser difundida. Embora o desenvolvimento da internet esteja relacionado diretamente à atividade governamental, é impossível negar que o fenômeno acabou por causar sérias dificuldades de regulação sobre a rede, especialmente pela incapacidade (ao menos inicial) do direito e seus institutos adequarem-se perfeitamente às dinâmicas líquidas da rede mundial de computadores.

2.1. A Dicotomia Átomo-Bit[6]?

A usual disciplina jurídica incidente por meio da edição de normas reguladoras, tendo seu *enforcement* baseado no monopólio da força estatal, viu-se relativamente incapacitada de recair sobre o ambiente digital. Conforme apresentam Johnson e Post (JOHNSON; POST, 1996, p.1367), a legitimidade e a aplicabilidade de normas reguladoras sobre as condutas humanas se viram degradadas em razão das comunicações globais promovidas pelas dinâmicas informacionais, portanto, a internet. A compreensão do direito e, por sua vez, das próprias estruturas de poder, passa necessariamente por uma abordagem de ciência política, com enfoque especial no território. Conforme expõem Firmino et al (2018, p. 390), o exercício do poder necessita (pelo menos necessitava) de sua manifestação física, demonstrada através do monopólio da força exercido sobre um povo dentro de um território delimitado, portanto, com uma ligação clara entre o Estado, o direito e o território.

[6] A expressão "dicotomia Átomo-Bit" foi firmada por Jean-François Blanchette no artigo "A material history of bits" (BLANCHETTE, 2011), no qual há a discussão da internet enquanto dotada de uma natureza dúplice, material e imaterial.

Brennen e Kreiss (2016, p.1-11) teorizam que a globalização e o progresso da técnica foram capazes de enfraquecer a noção clássica de soberania, ao ponto que o mundo, diante dos engendramentos técnicos da internet, tornou-se uno, sem distâncias, tudo isso alcançando incisivamente o Estado, especificamente com relação a sua capacidade legislativa e jurisdicional. A internet altera totalmente a ambiência regulatória usual, criando um espaço sem bases territoriais, rompendo com a histórica conexão entre o ambiente, em seu sentido geográfico, e o direito. Johnson e Post (1996, p. 1370) apresentam com clareza a total desvinculação entre o ciberespaço e as fronteiras físicas de um Estado, decorrendo dessa dissociação uma manifesta incapacidade regulatória, manifestada na ausência de bases materiais para o exercício coativo do direito.

Nas palavras de Roberto Kant Lima (LIMA, 2000, p.18):

> (o funcionamento da rede) não é plenamente conhecido por aqueles que a utilizam e, mais ainda são incipientes e exploratórias as formas de sua regulamentação. ... a tentativa de regulamentar um espaço destes- que produz, mesmo, um meio específico, o ciberespaço, anárquico, individualista, autônomo, com dimensões incontroláveis, em que os usuários se movem com enorme rapidez e se relacionam de forma profundamente igualitária- teria necessariamente de levar em consideração essas características, geradoras de uma multiplicidade de regras em constante reformulação, para entender aos aspectos profundamente dinâmicos das interações ali atualizadas.

Assim, entende o autor que regular a rede levando em conta o mundo dos átomos como paradigma, no qual há incidência razoável do direito e do poder organizacional do Estado, mostra-se como uma atitude incorreta, incapaz de ofertar soluções eficientes e adequadas à garantia de uma mínima segurança para esse ambiente. Torna-se necessário conduzir a regulação de uma atitude reflexiva do ambiente digital, levando em conta todas suas características, que diferem em muito dos padrões existentes no ambiente usual de vivência. Há todo um contexto diferente, uma estrutura com bases que divergem consideravelmente do meio físico, situação que demanda uma compreensão efetiva dessas bases e a produção de padrões regulatórios específicos, com atuações orientadas para o ambiente virtual, capazes de reagir de forma correta a toda a dinâmica típica do ambiente virtual.

Primeiro, pensar-se-ia que essa crise de legalidade definiria um ambiente de isenção, inexistindo capacidade de manifestação do poder estatal no âmbito da internet, aproximando-se muito daquilo que fora idealizado pelos teóricos sociais da internet nos anos 90. Assim, conforme expõem esses autores, seria esse um ambiente distante de mecanismos de controle

e, portanto, sendo perceptível uma clara distinção entre a regulação jurídica vigente no domínio dos átomos, no mundo real que nos cerca, e o mundo dos bits, o ambiente virtualizado. Antonio Jeová dos Santos (DOS SANTOS, 2001, p.11) apresenta bem a noção da internet enquanto ambiência de completa ausência de regras, demarcando seu caráter anárquico através dos vacúolos jurídicos ali reinantes, incapazes assim de estabelecer qualquer forma de regulação jurídica usual.

No entanto, partindo para uma abordagem mais profunda, a situação mostra-se oposta, havendo atuações adaptativas dos Estados e demais instituições para impor suas dinâmicas de controle sobre esse ambiente.

Conforme ressaltado por John Barlow (BARLOW, 1996) em sua Declaração de Independência do Ciberespaço, há o estabelecimento de legislações de controle e limitação de direitos dos usuários da rede, fazendo uso de agentes intermediários (provedores de internet, redes sociais, operadoras de telefonia móvel e fixa) para empreender o controle sobre a rede, sem contar com a dominação exercida diretamente sobre os cidadãos, no "âmbito do átomo". O exemplo marcante desse controle e, portanto, de um decaimento da dicotomia átomo-bit, é o mecanismo chinês de controle de fluxo, chamada "*The great chinese firewall*" e toda sua estrutura de suporte (FEIR, 1997), que se pauta no controle físico e na vigilância sobre os usuários, além do estabelecimento de ônus aos fornecedores de internet e grandes instituições, como exemplo, Facebook, Google e Youtube.

Firmino et al (2018, p.390) apresentam a ideia que o exercício do poder estatal ocorre por meio do controle de "porções de espaço" sobre as quais o Estado consegue exercer a sua autoridade. Essas porções de espaço seriam aqueles componentes físicos da cadeia de funcionamento da rede no qual é possível incidir fisicamente o poder estatal, lançando mão dos mecanismos usuais de regulação. Aprofundando muito bem a questão, Hood (1983) parte da ideia de que o Estado tem à sua disposição ferramentas "efetivadoras", que promovem o controle prático sobre a sociedade. Essas ferramentas manifestar-se-iam por meio de seu poder financeiro, do seu poder legal ou de sua organização (componentes materiais e humanos do Estado). Assim, para regular e exercer controle, pode o Estado lançar mão de qualquer desses institutos, como exemplo, podendo taxar excessivamente o acesso à rede para evitar seu acesso (poder financeiro), impor regras que limitam o acesso a certos sites (poder legal) e/ou lançar mão de meios físicos para impossibilitar o acesso (poder organizacional do Estado).

Portanto, por meio dos elos entre o mundo virtual e o mundo físico, que necessariamente existem, torna-se possível que o Estado exerça controle sobre o ambiente

digital, lançando mão das suas estruturas institucionalizadas de vigilância e dominação. Sem dúvida, o controle sobre as dinâmicas virtuais é extremamente dificultoso, no entanto, não podemos esquecer que inexiste a interface digital sem o aspecto físico que a provê, havendo total capacidade do controle ser exercido indiretamente, haja vista que o que ocorre no mundo físico quase sempre produz efeitos no ambiente digital, e vice-versa (FIRMINO et al, 2018, p.390).

Partindo dessa questão, Musiani et al (2016, p.2-4) entende que o Estado tem total controle tanto sobre o ambiente dos bits quanto sobre ambiente dos átomos, derrocando a dicotomia átomo-bit que reinava no pensamento dos juristas e sociólogos dos anos 90. Assim, afirmam os autores acerca do controle exercido pelo Estado sobre o ambiente digital, "*Ecosysten of institutions, laws and private ordering keeps the internet's infrastructure operational, as well as the enactment of public policy around this structure*[7]". Portanto, existem bases físicas e materiais da internet que permitem o estabelecimento de dinâmicas de controle e regulação sobre a internet, demonstrando claramente atuação primária do Estado buscando assumir seu poder nesse novo ambiente.

Ainda assim, há espaços no qual a atividade estatal e de seus prepostos não conseguem estabelecer regramentos e controle nos moldes usuais. A velocidade de expansão da internet faz com que a atividade regulatória do Estado não consiga seguir as dinâmicas ali engendradas, ainda mais quando tal atividade demanda todo um procedimento deliberativo, demonstrando assim a impossibilidade de controle total sobre esse ambiente. Nesses espaços, onde fica impossibilitado o exercício de controle institucionalizado pelo Estado, há o surgimento da chamada "alegalidade" (LAPRISSE, 2013, online). Nesses ambiente tidos como alegais inexiste um regramento jurídico suficiente para garantir a vigência da ordem jurídica, ou mesmo existem normas mas estas não conseguem disciplinar com especificidade as relações que ali são estabelecidas, pela adoção de leis inócuas por erros legislativos, por motivos políticos ou econômicos.

A alegalidade, portanto, denota um domínio digital livre, incapaz de sujeitar-se às dinâmicas diretas de controle do Estado, mas, além disso, conforme denota John Laprisse (2013, online), trata-se de um ambiente no qual o Estado tem a liberdade de agir conforme seus interesses, sem amarras legais que possam impedi-lo de lesionar direitos.

[7] Tradução dos autores "Um ecossistema de instituições, normas e disciplinas privadas que mantêm a operacionalidade da infraestrutura da internet, assim como permite a normatização por meio de políticas estatais sobre essa infraestrutura".

John Laprisse faz questão em demostrar que os Estados optam pela adoção de ambientes alegais, sobre os quais possam engendrar suas práticas tidas como ilegais caso fossem realizadas em um ambiente "normal" (2013, online), em especial, violações à privacidade dos usuários da rede. Portanto, há espaços em que é reconhecida a discrepância "átomo-bit", no qual o Estado não consegue ou não opta por promover a regulação, situações que levam os próprios entes e demais organizações com poder econômico e computacional a adotarem tais ambientes para albergarem suas atividades ilegais.

Assim, seguindo o que pensavam os teóricos dos anos 90 sobre a internet, essa contém uma parcela de seus domínios vigentes sob uma dinâmica de total liberdade, em razão da incapacidade de um controle eficaz por parte do Estado e seus prepostos. Nas palavras de Willian Mitchell (2000), essa visão romântica se aproximaria da chamada "*e-topia*", uma utopia acerca do ambiente virtual enquanto algo somente benéfico ao ser humano. Nesses ambientes, em razão da incapacidade de total sujeição às dinâmicas institucionalizadas de controle, o Estado e certas corporações os adentram e passam a engendrar dinâmicas de controle e vigilância massivas e ocultas, que se marcam pela ilegalidade, haja vista a "alegalidade" e o anonimato que ali vige. Portanto, a dicotomia marca-se em razão de uma reestruturação dos meios de controle e das suas manifestações no ambiente virtualizado, apresentando mudanças marcantes quando comparados com o controle exercido no ambiente físico.

Dessa forma, podemos afirmar que há e não há uma dicotomia "átomo-bit". Ao mesmo passo em que as estruturas de controle estatal conseguem ser engendradas de forma eficaz sob as dinâmicas virtuais institucionalizadas e reguladas, por meio da incidência de poder indiretamente através de agentes intermediários, denotando um controle semelhantemente exercido no domínio do bit e do átomo, vemos também que há uma reestruturação dos meios de controle e vigilância, que possibilitam o exercício do poder de forma muito mais intensa por parte do Estado e de corporações envolvidas com o ambiente digital, indo além até mesmo da legalidade. Assim, o poder de controle exerce-se nos dois domínios, no entanto, o domínio do bit abriga formas de controle robustas e ocultas, reconstruídas aos moldes do ambiente em que se desenvolvem, denotando assim uma diferença marcante com relação ao domínio físico.

Essa dicotomia e "não-dicotomia" engendra uma profunda crise de legalidade, no qual o direito, enquanto limitação à atuação estatal violatória e mecanismo de regulação das relações sociais, tem o seu *enforcement* gravemente abalado, seja pelo seu uso enquanto mecanismo de controle indireto (através de agentes intermediários), totalmente cooptado

pelos interesses econômicos e políticos que o cercam, seja pela utilização de seus vacúolos, por parte do Estado, para o engendramento das práticas de controle, opondo-se diretamente às diretivas constitucionais que regulam a atuação estatal.

3. PRIVACIDADE DIGITAL E O CASO *WIKILEAKS*

O vazamento das práticas de espionagem por meio da plataforma *Wikileaks* trouxe à tona a questão da vigilância massificada por intermédio da tecnologia e das práticas digitais, apresentando especificamente os meios sobre os quais se pautam as atividades de espionagem privada por parte dos Estado e grandes corporações. Importante aqui ressaltar que a partir do ano de 2013 o mundo já vinha sendo alertado sobre os perigos da vigilância globalizada, efetivada pelas vias digitais, com os vazamentos feitos por Edward Snowden, apresentando mecanismos governamentais e empresariais de vigilância.

A garantia da privacidade, enquanto direito humano positivado nas cartas constitucionais da maioria dos países democráticos, não consegue alcançar semelhante tutela quando adentramos no mundo dos bits, um ambiente tido como alegal, no qual há o engendramento de práticas ilícitas por todos os usuários, inclusive aqueles institucionais. Portanto, fica fácil, diante da breve contextualização feita, visualizar que a privacidade digital sofre expressiva limitação, sendo quase inalcançável uma tutela jurídica semelhante àquela oferecida para o mundo dos átomos (que já é deveras insuficiente). Nas palavras de Góis Júnior (GÓIS JR, 2002, p.p.95), a internet mostra-se como um ambiente propício à violação dos direitos de privacidade, em razão direta da vastidão de seus meios, do alto grau de anonimato dos usuários e da dificuldade regulatória

A sociedade atual, envolta em um número massivo de informações, encontra-se inserta em uma dinâmica constante de invasões de privacidade, seja pela atuação ativa dos Estados e corporações, seja pela exposição voluntária dos usuários. Nesse âmbito, o caso *Wikileaks* conseguiu confirmar as tendências que já estavam nas ideias dos teóricos da internet, apresentando com clareza diversas das dinâmicas de controle e vigilância empreendidas. Conforme ressalta Steve Mansfield-Devine (MANSFIELD-DEVINE, 2018, p.15), fica clara a fraqueza do modelo democrático de direito e sua estrutura jurídica quando o comparamos com a robusteza do ambiente virtual da internet, um ambiente quase ausente de regulações quando nos referimos a garantia de direitos dos usuários, onde reina a alegalidade e, assim, o poder daqueles com maior capacidade programacional. Sem dúvida, conforme fora

apresentado, há regulações diretas e indiretas providas sobre o ambiente digital, denotando formas de controle e táticas de vigilância social, no entanto, ao abordarmos meios formais e concretos de disciplina jurídica dos direitos dos usuários da rede, nos deparamos com quase uma total vacância legislativa.

Segundo John Palfrey e Jonathan Zittrain (PALFREY; ZITTRAIN, 2011, p.1210-1211) essa ausência regulatória sobre os direitos humanos no âmbito digital está associada à duas problemáticas, à existência de questões de ordem técnica, que impedem uma efetiva incidência da norma protetiva sobre esse domínio, e à existência de interesses econômicos e políticos que impedem a tutela e a efetivação desses direitos. Em especial, devido a natureza da rede, grande parte das lesões se desenvolvem no âmbito dos direitos de personalidade, relacionadas à privacidade, intimidade e à livre expressão dos indivíduos nos ambientes virtuais.

As corporações digitais, desenvolvedoras, armazenadoras e gerenciadoras de dados, se vêm diretamente imersas nessas dinâmicas de vigilância, no qual exercem controle ou mesmo disponibilizam aos órgãos fiscalizadores ferramentas e meios programacionais para supervisionar esses dados, destinados, primeiramente, a cumprir com obrigações jurídicas junto aos Estados, mas também com finalidades econômicas, captando informações com objetivos próprios. É necessário considerar a exploração comercial de informações pessoais como parte substancial do faturamento das corporações digitais e comunicações, sem tirar de mente a possibilidade também da venda destas informações por funcionários dessas corporações, em proveito próprio. Um exemplo das práticas de vigilância pelas corporações digitais são os termos de serviço do Linkedin, que pertence à Microsoft, que preveem que todas as informações colocadas na plataforma como pertencentes à Microsoft, com possibilidade uso econômico dessas (MARTÍNEZ-BEJAR; BRÄNDLE, 2018, p. 144).

Tomando como exemplo os Estados Unidos da América, há uma tendência institucionalizada de quebra dos deveres de sigilo com relação às informações pessoais confiadas a pessoas ou corporações, em razão da chamada Teoria do Terceiro (*third-party doctrine*), já consagrada na Suprema Corte estadunidense[8]. Segundo essa teoria, aquele indivíduo que oferece suas informações voluntariamente a um terceiro (que não estaria ligado diretamente com um dever de sigilo) não teria direito de esperar que sua privacidade seja mantida por este último, de forma que as empresas que recebem voluntariamente dados de seus clientes não têm o dever de manter sigilo sobre estes, não sendo em nenhum momento

[8] Caso firmado no leading case United States *v.* Miller (ESTADOS UNIDOS DA AMÉRICA, 1976).

esperado que essas informações sejam sujeitas à privacidade (PELL; SOGHOIAN, 2014, p.19-21).

As informações repassadas a terceiros não têm sua privacidade e intimidade garantidas, geralmente informações essas captadas mediante termos de cessão de informações que figuram como contratos de adesão, no qual serão necessariamente captadas caso o usuário queira usufruir do domínio ou serviços fornecidos por este terceiro, situação esta que leva, como retratado nos vazamentos realizados pelo *Wikileaks* no ano de 2017 e Edward Snowden no ano de 2013, as grandes corporações do ramo digital fornecerem informações pessoais dos usuários aos governos de todo o globo, que as utilizam para estabelecer vigilância sobre o âmbito privado dos indivíduos.

Tomando como exemplo os Estados Unidos da América, Ryan Calo (CALO, 2012, p.1030-1032) ressalta que a quebra de privacidade no ambiente digital, em razão da vacância de normas protetivas sobre o ambiente digital, ocorre mediante simples requisições das agências governamentais, independentemente da existência de autorização judicial, sendo engendrada essas dinâmicas de formas mais expressivas após 11 de setembro de 2001, que com o suporte jurídico do Ato Patriótico estabeleceu mecanismos de vigilância pautados na detecção de perigos ao Estado e à ordem econômica vigente.

3.1. Quebra da privacidade na rede

A quebra da privacidade mostra-se como um fenômeno histórico, presente desde sempre nas dinâmicas de vivência das sociedades humanas, recebendo a devida tutela jurídica somente após o estabelecimento das bases primogênitas de direitos humanos. A ofensa à privacidade apresenta-se enquanto condução de informações típicas do âmbito de intimidade à esfera pública, portanto, a condução do conhecimento privado para pessoas externas ao círculo de confiança do detentor das informações, havendo um claro direito do indivíduo ser deixado em paz (*right to be let alone*) e ter sua intimidade e honra reservados.

Conforme apresentam Warren e Brandeis (WARREN; BRANDEIS, 1890) o direito à privacidade (lato sensu) compreenderia a privacidade (stricto sensu), enquanto direito de ter controle sobre quaisquer informações privadas que possam de qualquer forma afetar psicologicamente o indivíduo fonte, e o direito à intimidade, enquanto direito de gozar a vida sem qualquer embaraço, distante dos olhos de terceiros. Tratam-se, assim, de direitos apartados do direito de propriedade e da liberdade, assim, direitos humanos autônomos,

relacionados diretamente à essência humana. Dessa forma, o direito à intimidade estaria relacionado à confusão entre as esferas privada e pública, reverberando tal confusão sobre a privacidade (stricto sensu) a partir do momento em que é potencial alguma lesão à honra e à imagem do indivíduo fonte das informações, portanto, capaz de afetar a sua personalidade.

Rosângela Miranda (MIRANDA, 1993, p.44) interpreta uma série de fatos sociais e políticos identificados como fatores incisivos na definição do conflito entre a esfera privada e a esfera pública, conflito esse que marca a violação da privacidade. Inicialmente, é constatado um traço natural ao ser humano como ponto inicial da compreensão da crise da privacidade, a curiosidade, manifestada no intuito recorrente de conhecer aquilo que está além de seus conhecimentos, adentrando muitas vezes na esfera privada. Adentrando em questões políticas, outro ponto chave da derrocada da privacidade é encontrado no totalitarismo estatal, objetivando o estabelecimento de formas de controle social direto e indireto. Abordando sob uma ótica sociológica, é impensável deixar de trazer à discussão a atuação niveladora da cultura de massas, que impõe aos indivíduos uma ostentação cada vez maior de suas particularidades, visando descontruir a singularidade por meio da afirmação do comum.

Diante de todos os fatores enumerados pela autora, aponta-se a revolução tecnológica como fenômeno catalizador da corrosão da intimidade e privacidade, no qual há o desenvolvimento e aplicação de mecanismos cada vez mais capazes de romper as já esmaecidas divisas entre a esfera pública e privada. A revolução tecnológica, como abordada pela autora, não tem como referência somente a atual técnica informacional sobre a qual nos pautamos, mas também todas os outros desenvolvimentos técnicos que atuam e aturaram de certa forma sobre a privacidade, como o caso da explosão jornalística do fim do século XIX, cujos abusos cometidos sobre a privacidade levaram Warren e Brandeis promover sua teorização, elencando o fenômeno da "massificação jornalística" enquanto problema principal a ser resolvido pela teoria do direito à privacidade. A trama de Henry James, The Reverberator, consegue expressar com clareza o fervor jornalístico que se desenvolvia na época, demarcando a necessidade recorrente de conhecimento de fatos personalíssimos devidamente noticiados em colunas jornalísticas de fofoca, levando a reiteradas ofensas à privacidade por parte dos jornalistas.

Contextualizando a questão junto à atual dinâmica técnica, é possível perceber a sua escalada expressiva, acompanhada de perto pelo incremento das possibilidades de ofensas à privacidade. A internet permitiu o estabelecimento de meios mais eficientes e menos incisivos de acesso às informações íntimas, seguindo de perto aquilo que já fora traçado anteriormente com o incremento da técnica jornalística no final do século XIX. Agora, de forma cotidiana,

inserimos “tabloides” dentro de nossos bolsos e casas, fornecemos bytes e bytes de informações que, no seu devido destino, são utilizadas para fins mercadológicos e de controle. A técnica se incrementou, os fins alteraram-se mas, acima de tudo, as bases de violação sobre a privacidade permanecem estáveis e regulares.

A quebra da privacidade nos ambientes virtuais apresenta-se como uma problema grave muito bem afastado da discussão pública e até mesmo da academia, implicando em reiteradas violações de direitos humanos através de estruturas alegais sobre as quais atuam Estados e corporações econômicas. Os indivíduos imersos nas sociedades digitalizadas são sujeitos constantemente a observações, escaneamentos, digitalizações, dentre outras formas de lesão à privacidade e liberdade, tudo isso no intuito de facilitar o reconhecimento, a identificação e o aproveitamento mercadológico, visando obter um nível mínimo de controle social e econômico.

3.2. As denúncias de Espionagem expostas pelo site *Wikileaks*

Os Estados, enquanto alvos principais das acusações veiculadas pelo Wikileaks, apresentam-se como principais violadores da privacidade, lançando mão de inovadores métodos de captação de dados, atuando sob a proteção de ambientes digitais alegais para estabelecer mecanismos de controle e dominação, muitas vezes transvestidos enquanto mecanismos de segurança e prevenção à criminalidade. A internet, fruto direto das pesquisas do Departamento de Defesa Estadunidense na Arpanet, mostra-se marcada pelas dinâmicas de ruptura da privacidade desde seu surgimento, estando o Estado amparado com todo o aparato ferramental e humano por trás do desenvolvimento e funcionamento desse novo mecanismo de comunicação. Em uma visão claramente Elluliana (ELLUL, 1968, p.290-296), é visível que a técnica informacional surge já dentro do Estado, como um incremento das práticas de dominação.

Em casos como o Atentado à maratona de Boston em 2013, no qual houve a utilização massiva de informações de vigilância (muitas delas ilícitas, realizadas sob o manto da alegalidade), fica visível o poder de vigilância do Estado. Os casos expostos por Assange e Snowden são ainda mais demonstrativos, abrindo ao mundo uma série de informações contendo métodos, até então impensáveis, pelos quais há a obtenção do acesso à intimidade dos cidadãos. As informações são obtidas através de mecanismos próprios de captação, acobertados pelo anonimato e ausência de legalidade vigente sobre parte do espaço digital, ou

mediante requisições destinados às corporações digitais, que os fornecem independente do preenchimento dos requisitos legais, de forma totalmente externa ao devido processo legal. Todos os procedimentos legais são omitidos durante a obtenção dessas informações personalíssimas, inexistindo rastros capazes de responsabilizar o Estado ou mesmo as instituições fornecedoras, havendo a operação por meio de mecanismos ocultos e de difícil rastreamento, conforme bem mostraram os documentos expostos por Assange.

Analisando as denúncias veiculadas no site Wikileaks, nos deparamos com casos como o de participação em redes massivas de vigilância, realizados pelos Estados Unidos da América, Canadá e Reino Unido, diretamente sobre os usuários da rede e de telefones celulares (WIKILEAKS, 2014, online), casos de revelação não autorizada de comunicações (PELL; SOGHOIAN, 2014, p.23-26), desenvolvimento de ferramentas e centros para vigilância massiva na rede e espionagem (WIRED, 2014, online), vazamento de informações restritas às bases de registro do Estado (PELL; SOGHOIAN, 2014, p.27-29), controle dos fluxos humanos por meio de checagens prévias de dados digitais, práticas estas realizadas pelos Estados Unidos da América. Além disso, há casos de vigilância massiva por meio de câmeras, ocorridos na Espanha e França (LIPPERT; NEWELL, 2016, p.113), além de registro de dados biométricos, na China.

Os documentos vazados no site *Wikileaks* também narram as formas pelas quais grandes companhias captam ilegalmente informações, chegando a fornecê-las às agências de segurança, rompendo claramente com a privacidade dos usuários. Dentre diversas acusações, encontram-se aquelas que afirmam que empresas como Amazon, Apple, Facebook, Google, Microsoft, Skype, Yahoo, Youtube, CNN, FOX, Paypal, Visa e American Express realizam tais práticas de fornecimento "às escuras" de informações de seus usuários (GELMAN,2013, online). Empresas como a AT&T e AOL possuem em suas políticas de privacidade medidas de suporte à atividades de captação ilícita de informações por parte do Estados e suas agências (MÁRTINEZ-BEJAR; BRANDLE, 2018, p.145). Corporações como Google, Facebook, Skype, Twitter , Amazon, Apple, Mastercard, Visa, Paypal, AOL, Microsoft , dentre outras, são comprovadamente participantes de redes internacionais de vigilância (WARREN, 2012, online), (GELMAN, 2013, online). As empresas Facebook e Instagram realizam a apropriação de informações, para fins comerciais, de informações colocadas pelos usuários na plataforma, assim como a venda de localização de usuários por parte da empresa Tomtom (DAILY MAIL, 2011, online).

Importante ressaltar que, além dessas práticas, grandes corporações têm enorme influência na atividade legislativa dos Estados, atuando diretamente por meio de *lobbies* e

cooptação de figuras políticas, tudo isso objetivando a garantia de seus interesses dentro da esfera jurídica. Como exemplo, vale citar o *lobby* feito pelo Google, Facebook e Twitter para evitar a aprovação da Lei de privacidade de adultos e crianças do Estado da Califórnia em 2011, que buscava evitar qualquer uso de informações sem o aval de seu proprietário (MACGREEVY, 2011).

É necessário entender que as corporações digitais, enquanto agentes com capacidade técnica e financeira para desenvolver e gerenciar parcelas da rede mundial de computadores e seus mecanismos, possuem expressivo poder dentro da rede, atuando por meio de esferas alegais que mascaram suas atividades ilícitas sobre a privacidade, através de papéis intermediários nos fluxos de informação, enquanto *longa manus* do Estado e de sua regulação, com acesso privilegiado a tais informações, ou mesmo, de forma contumaz, violando a privacidade com o "aval" do Estado, que se utiliza dessa situação de ilegalidade para também ter acesso à esses dados.

As informações obtidas por essas grandes corporações, em sua grande maioria, formam um fluxo invisível destinado diretamente ao Estado, que as recebe e tira proveito sem ao menos questionar as formas de obtenção e as suas claras violações aos direitos fundamentais dos usuários. Além disso, é frequente também a monetização dessa fluxo de dados privados, por meio de fornecimento de serviços analíticos, de pesquisas e de publicidade direcionada. O escândalo dos dados privados utilizados para fins políticos por intermédio da *Cambridge Analitics* expressa bem esse fenômeno, no qual o Estado e seus agentes fazem uso de serviços de captação e processamento de informações obtidas irregularmente, havendo inclusive o uso dessas técnicas para alterações nas dinâmicas eleitorais.

Houve um incremento nas formas de vigilância e mercantilização de informações sensíveis captadas pela rede, acompanhado diretamente por uma maior passividade dos usuários da rede, seja pela necessidade cada vez maior de acesso à rede para a vivência social (refletindo uma cultura de massa) e profissional, seja pela dependência psicológica ou simples acomodação. Casos anteriores, como o da empresa *Double Click*, fundada no ano de 1996, mostravam reações muito mais contundentes dos usuários diante de práticas de captação e capitalização de informações pessoais por meio da rede (VIEIRA,2002, p. 83), reações estas nunca mais vistas, mesmo diante de fenômenos gritantes, como as exposições do *Wikileaks*.

Se algo está na esfera digital, isso não é efetivamente privado. O *token* digital de cada pessoa é totalmente vigiado, devendo ser afirmado que a capacidade de reagir dos cidadãos diante de tamanho controle é limitada, ainda mais quando estamos imersos em uma

dinâmica algocrática[9] (AANESH, 2002), que determina previamente os caminhos e os destinos de nossas condutas.

José Adércio Leite Sampaio (SAMPAIO, 1998, p.470) pondera:

> A total transparência do indivíduo aos olhos do Estado e das empresas, detentoras do monopólio da informação, agudiza a concentração do poder, fragiliza o controle que deve ser exercido pela sociedade- e não, sobre a sociedade- favorecendo as discriminações e o conformismo social e político"

Os cidadãos, diante do controle da tecnologia, seja ela softwares, hardwares ou o próprio acesso à internet, estão em uma posição de hipossuficiência, especificamente técnica, em razão da necessidade de sujeitarem-se às dinâmicas de usurpação de dados que é realizada pelos "nós" dominantes da rede. Essas corporações e Estados efetivam a coleta desses dados, seja de forma semi-voluntária, sendo a permissão a condição necessária para a utilização de certos ambientes virtuais, seja pelo engendramento de práticas de efetiva vigilância, como aquelas muito bem narradas nos documentos disponibilizados no *Wikileaks*.

CONSIDERAÇÕES FINAIS

Ainda na década de 70, atrelado às visões neonatais da internet, Paul Armer (1975, p.13) já ressaltava o inerente perigo de expansão dos mecanismos vigilância e controle no mesmo ritmo do incremento da técnica, afirmando que isso traria enorme risco à privacidade e à liberdade humana. Para evitar que fosse estabelecida uma dinâmica Orwelliana de controle, era necessário que todos estivessem constantemente preocupados e alertas com esses riscos, ensejando uma atuação política e bem informada da população no sentido de não se conformar aos meios tecnológicos "anestesiantes", de forma a evitar totalmente a criação de um ambiente onde a cidadania não tivesse o controle como condição necessária.

As pessoas têm se tornado acostumadas com as novas tecnologias de controle das comunicações e informações, havendo a delegação cada vez maior de funções humanas a tais sistemas, abrindo espaço para essas formas de vigilância. Seguindo a dinâmica humana sobre a técnica, há o estabelecimento de uma visão fáustica sobre as inovações digitais e informacionais (MARTINS, 2012, p.61), ocorrendo o entorpecimento dos indivíduos no sentido de que todos os benefícios trazidos pela tecnologia serão eternos e sem efeitos

[9] Regime de controle promovido pelos algoritmos.

colaterais, não alcançando uma finitude ou qualquer malefício. Todo obscurecimento trazido por essa condição fáustica levou a uma imersão absurda da sociedade e do indivíduo nas dinâmicas informacionais, com a criação da internet das coisas, conectividade constante à rede e uma exposição pública incessável, suplantando por trás de seus benefícios toda uma carga de dominação e controle exercida pelas instâncias de poder.

Indo além, o efeito encantatório das tecnologias informacionais é tamanho que sempre houve questionamentos acadêmicos[10] dos problemas que poderiam ser causados sobre a privacidade e liberdade humana com o engendramento desses mecanismos, no entanto, estes nunca receberam a devida atenção ou chegaram à grande massa de usuários da rede, que permanecem confiando plenamente na estrutura da internet e depositando informações. Questionando a abordagem "fáustica" da tecnologia informacional, é possível afirmar que os benefícios trazidos pela internet surgiram concomitantemente com as medidas de controle e dominação dos Estados e corporações, havendo uma sensação de que esses benefícios nunca seriam suplantados por malefícios, que já estavam presentes mas muito bem maquiados. A anestesia promovida pela técnica, assimilada a uma massificação psicológica (ELLUL, 1968, p.419) consegue impor uma carga de dominação nunca antes vista, engendrada em um sistema eficiente que, apesar de todas as exposições, permanece tendo adesão dos usuários da rede.

Atuando como o flautista de Hamellin, a internet e suas tecnologias correlatas encantou a todos enquanto nos conduz à perdição, estando nós imersos nesses ambientes digitais sem a capacidade de questionar e se opor aos malefícios que foram, estão sendo e serão causados.

Embora o direito se debruce sobre a questão da privacidade, como um todo, albergando esta enquanto uma condição básica à dignidade humana, tutelada constitucionalmente na maioria dos países de tradição jurídica ocidental, nota-se que há enorme dificuldade de efetivação destes direitos no ambiente virtual, por uma gama de fatores. Inicialmente, como abordado antes, a existência de espaços alegais, frutos diretos da expansão crescente da rede e a minguante capacidade regulatória do Estado, impede a atuação de mecanismos efetivos de tutela dos direitos de privacidade.

Assim, as lesões à privacidade ocorrem no ambiente alegal em razão da tolerância estatal, que consente com a obtenção e utilização desses dados diante dos seus interesses políticos e estratégicos, muito bem garantidos também através desses domínios isolados da

[10] Paul Armer já falava sobre isso no ano de 1975, pouco tempo após o nascimento da internet.

visão geral do público. Além disso, há a possibilidade da criação de espaços alegais muito além do conhecimento estatal, permitindo que corporações desenvolvam práticas ilícitas sem ao menos serem vislumbradas. Estando a efetividade prática do direito diretamente vinculada à capacidade de intervenção do Estado (ao menos nos moldes atuais), os ambientes alegais, onde são desenvolvidas as obtenções de dados sensíveis, tornam impossível a garantia dos direitos de privacidade e também dos demais direitos humanos.

O Estado, quando abordado sob essa óptica, toma conotações leviatanescas, opondo-se totalmente às bases jurídicas limitadoras de sua atuação. Torna-se impossível pensar no Estado enquanto vinculado à legalidade e à norma constitucional quando nos deparamos com a clara realidade, que apresenta manifestas violações praticadas pelo Estado contra os direitos fundamentais, podendo visualizá-las nas diversas denúncias feitas através do domínio *Wikileaks*. Torna-se uma hipocrisia reiterar o dogma da privacidade, manifestado na necessidade de autorização judicial para acessar dados privados, quando o Estado e grandes corporações, atuando sob esferas de alegalidade, têm acesso irrestrito a informações, captando-as constantemente sem qualquer embaraço.

Portanto, fica bem definido que o uso reiterado das tecnologias informacionais para infringir a privacidade vem sendo encarado com passividade pela população, com uma expansão frenética da chamada internet das coisas e da imersão na rede mundial de computadores, situação esta que encoraja ainda mais o estabelecimento de métodos e ferramentas de quebra da privacidade e estabelecimento de modelos de controle e vigilância. A expansão da técnica informacional ocorre em uma velocidade inacreditável e, de forma conjunta, há a expansão dos mecanismos de controle e vigilância exercidos pelo Estado e grandes corporações do ramo digital. As denúncias veiculadas por Assange no site *Wikileaks*, especificamente nos documentos *Spy Files e Vault 7*, apresentam uma prévia das formas usuais de vigilância e controle exercidas sobre a sociedade por intermédio da internet e suas ferramentas, indicando uma clara convergência do exercício do poder, antes manifestado sob a forma organizacional, assim, em medidas físicas, agora manifestado por meio da informação e seu controle, exigindo que para o alcance de objetivos diversos haja a reiterada quebra da privacidade dos usuários da internet.

REFERÊNCIAS

AANESH, Aanesh. **Technogically Coded Authority:** The Post-Industrial Decline in Bureaucratic hierarchies. *In*: International Summer Academy On Technology Studies, jul. 2002, Deutschlandsberg (Aústria). **PAPEL DA CONFERÊNCIA** […] . Deutschlandsberg: IFF/IFZ, 2002. Disponível em : http://web.stanford.edu/class/sts175/NewFiles/Algocratic%20Governance.pdf . Acessado em 01 maio 2019.

ARMER, Paul. **Computer Technology and Surveillance.** Santa Clara (EUA): Center for Advanced Studies in the Behavioral sciences, 1975. Disponível em : https://stacks.stanford.edu/file/druid:zf198qx6952/zf198qx6952.pdf . Acessado em 25 maio 2019.

BARLOW, John Perry. **A Declaration of Independence of Cyberspace.** 8 fev. 1996. Disponível em: https://www.eff.org/cyberspace-independence . Acessado em 09 maio 2019.

BLANCHETTE, Jean-François. A Material History of bits. **Journal of the American Society for Information Science and Technology**, Nova Iorque, v.62, n.6, jun. 2011, p.1042-1057.

BRENNEN, J. Scott; KREISS, D. Digitalisation. In: JENSEN, K. B. et al (Eds.). **The International Encyclopedia of Communication Theory and Philosophy.** Nova Jersey (EUA): John Willey and Sons, 2016. Disponível em: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118766804 . Acessado em 10 maio 2019.

CALO, Ryan. Against notice skeptism in privacy (and Elsewhere). **Notre Dame Law Review**, Paris, v.87, n.3, 2012, p.1027-1072.

DAILY MAIL. Now Tomtom apologises for selling customer satnav data, which police used to set up speed traps. **Daily Mail**, 28 de abril de 2011. Disponível em: https://www.dailymail.co.uk/sciencetech/article-1381491/TomTom-apologise-selling-customer-satnav-data-used-police-speed-traps.html . Acessado 30 maio. 2019.

DOS SANTOS, Antonio Jeová. **Dano Moral na internet**. São Paulo: Método, 2001.

ELLUL, Jacques. **A Técnica e o Desafio do Século**. Rio de Janeiro: Paz e Terra, 1968.

ESTADOS UNIDOS DA AMÉRICA. SUPREMA CORTE. **USA v. Miller**. Julgado em 12 de janeiro de 1976. Disponível em: https://supreme.justia.com/cases/federal/us/425/435/ . Acessado em 30 maio 2019.

FEIR, Scott. E. Regulations restricting internet access: attempted repair of rupture in China's great wall restraining the free exchange of ideas. **Pacific Rim Law and Policy Journal**, Seattle (EUA), v.6, n.2, 1 mar. 1997, p.361-389.

FIRMINO, Rodrigo; MELGAÇO, Lucas; KLOZA, Dariusz. The spatial bonds of Wikileaks. **Government Information Quarterly**, [*s. l.*], v.35, 2018, p.389-397.

GELMAN, Barton. US, British Intelligence mining Data from nine U.S Internet Companies in broad secret program. **The Washington Post**, 7 de junho de 2013. Disponível em: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-

internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html . Acessado 15 maio. 2019.

GÓIS JÚNIOR, José Calda. **O Direito da era das redes.** São Paulo: Edipro, 2002.

HOOD, C. C. **The Tools of Government.** Londres: Macmillan, 1983.

JOHSON, David R.; POST, David G. Law and Borders: the rise of Law in Cyberspace. **Stanford Law Review**, Stanford (EUA), v. 48, 1996, p. 1367-1404.

LAPRISSE, John. **US National Security Agency Surveillance:** A Problem of Alegality. 10. Jun. 2013. Disponível em : http://ohrh.law.ox.ac.uk/us-national-security-agency-surveillance-a-problem-of-allegality/ . Acessado em 10 maio 2019.

LIMA, Roberto Kant. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000.

LIPPERT, Randy K.; NEWELL, Bryce Clayton. Debate introduction: the privacy and surveillance implications of police body cameras. **Surveillance and Society**, Windsor (Canada), v. 14, n.1, 2016. p. 113-116.

MACGREEVY, Patrick. Online privacy bill fails to pass California Senate. **Los Angeles Times**, Los Angeles, 28 de maio de 2011. Disponível em: https://www.latimes.com/local/la-xpm-2011-may-28-la-me-social-networking-20110528-story.html . Acessado: 04 maio 2011.

MANSFIELD-DEVINE, Steve. Hacking democracy: abusing the internet for political gain. **Network Security**, Amsterdam, v. 2018, n.10, out. 2018, p.15-19.

MARTINS, Hermínio. **Experimentum Humanum**: civilização tecnológica e condição humana. Belo Horizonte: Fino Traço, 2012.

MARTÌNEZ-BEJAR, Rodrigo; BRÄNDLE, Gaspar. Contemporary technology management practices for facilitating social regulation and surveillance. **Technology and Society**, Amsterdam, v.54, 2018, p.139-148.

MIRANDA, Rosângela. **A transformação da intimidade.** São Paulo: Unesp, 1993.

MITCHELL, Willian John. **E-topia**: urban life, jim-but not as we know it. Cambridge, MA: MIT Press, 2000.

MUSIANI, F. et al. **The turn to infrastructure in internet governance.** Nova Iorque: Macmillan, 2016.

PALFREY, John; ZITTRAIN, Jonathan. Better data fot a better internet. **Science**, v.334, n.6060, dez. 2011, p.1210-1211.

PELL, Stephanie K; SOGHOIAN, Christopher. Your secret sting-ray's no secret anymore: the vanishing government monopoly over cellphone surveillance and It's impacts on National security and consumer privacy. **Harvard Journal of Law and Technology**, Cambridge (EUA), v.28, n.1, mar/jun., 2014, p.1-76.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1998.

SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação. **A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE CONCRETIZAÇÃO DA AUTONOMIA PRIVADA EM UM MUNDO CADA VEZ MAIS TECNOLÓGICO**. Revista Juridica, [S.l.], v. 3, n. 56, p. 354 - 377, jul. 2019. ISSN 2316-753X. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581/371371972>. Acesso em: 26 abr. 2020. doi:http://dx.doi.org/10.21902/revistajur.2316-753X.v3i56.3581.

VIEIRA, Sônia Aguiar do Amaral. **Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos**. São Paulo: Juarez de Oliveira, 2002.

WARREN, Christina. Revealed: The FBI wants to monitor Social Media. **Mashable,** 26 de junho de 2012. Disponível em: https://mashable.com/2012/01/26/fbi-social-media-monitoring/#jTXNR821WaqZ . Acessado em 29 maio 2019.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, Cambridge (EUA), v.4, n.5, 15. dez. 1890, p.193-22.

WIKILEAKS. **The Spy Files.** 2014. Disponível em: https://wikileaks.org/the-spyfiles.html . Acessado em 20 maio 2019.

WIRED. **Edward Snowden: The untold story**. 2014. Disponível em: https://www.wired.com/2014/08/edward-snowden/ . Acessado em 20 maio 2019.

ZAKON, Robert Hobbes. **Hobbes' Internet timeline**. Disponível em : https://info.isoc.org/guest/zakon/internet/history/hit.html . Acessado em 20 maio 2019.