UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS

ESCOLA DE CIÊNCIAS JURÍDICAS

CURSO DE DIREITO

JOÃO MARCELO DE AMORIM BAPTISTA

A SURVEILLANCE NO ÂMBITO POLÍTICO-ECONÔMICO E SEUS REFLEXOS CONSTITUCIONAIS

Rio de Janeiro – RJ

2015

JOÃO MARCELO DE AMORIM BAPTISTA

SURVEILLANCE NO ÂMBITO POLÍTICO-ECONÔMICO E SEUS REFLEXOS CONSTITUCIONAIS

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Jurídicas da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. ANTONIO CESAR PIMENTEL CALDEIRA

Rio de Janeiro

2015

Dedico este trabalho aos meus pais, que me ensinaram desde cedo a importância do estudo e me mostraram que com esforço podemos chegar aonde quisermos.

RESUMO

Este trabalho tem como escopo estudar o impacto do fenômeno da Surveillance na vida das pessoas, questionando sua validade jurídica e seus impactos às garantias individuais. Primeiramente, através de uma análise histórica desta prática, será abordada a evolução conceitual do termo – passando por Foucault, Orwell e outros. Em seguida serão abordados, ponto a ponto, os princípios constitucionais violados, suas origens históricas e quais institutos eles visam proteger. O estudo diferenciará os objetivos procurados com a aplicação de seus meios. Enquanto o Estado utiliza a Surveillance como modo de controle social, as corporações buscam seus interesses econômicos. Com o uso de dados estatísticos, iremos avaliar o alcance deste mecanismo e como o emprego de métodos tecnológicos avançados permitiu a expansão de sua prática ao redor do globo e como é seu funcionamento empírico. O estudo também apresenta dados sobre a legislação em diversos países e tratados internacionais e como a sociedade vê os efeitos da Vigilância a partir do século XXI. O trabalho buscará também apresentar os casos mais emblemáticos recentes de exposição da Surveillance – Edward Snowden e Julian Assange - e, brevemente, analisará como a sociedade tem procurado responder à altura com o que ficou conhecido como “Sousveillance”.

Palavras-chave: Surveillance, Vigilância, Controle Social, Garantias, Direitos.

ABSTRACT

The scope of this paper is to study the impact of the phenomenon of Surveillance in people's lives, questioning its legality and its impacts to individual guarantees. First, through a historical analysis of this practice will be addressed conceptual evolution of the term – through Foucault, Orwell and others. Then will be covered, point to point, the constitutional principles violated, their historical origins and which institutes they aim to protect. The study will differentiate the objectives sought through the application of its means. While the State uses the Surveillance as a means of social control, corporations seek their economic interests. With the use of statistical data, we will assess the scope of this mechanism and how the use of advanced technological methods enabled the expansion of the practice around the globe and how it works. The study also presents data on the legislation in various countries and international treaties and how society sees the effects of surveillance from 21ST century. The work will also present the most emblematic cases of recent exposure of Surveillance – Edward Snowden and Julian Assange - and, briefly examine how the society has sought to respond to with what became known as "Sousveillance".

Key-words: Surveillance, Social Control, Guarantees, Rights.

SUMÁRIO

1. INTRODUÇÃO

Inicialmente, devemos esclarecer que embora a tradução de Surveillance – Vigilância – seja aceitável, ela não engloba o conceito intrínseco desta palavra no inglês. Nas palavras de Schopenhauer (2009, p. 149-150):

> *Às vezes ocorre também que uma língua estrangeira expresse um conceito com uma sutileza que a nossa própria língua não lhe dá, de modo que o pensamos apenas naquela língua com tal sutileza. Com isso, cada pessoa que busca uma expressão exata de seu pensamento usará a palavra estrangeira, sem se importar com a algazarra dos puristas pedantes. Em todos esses casos, não é exatamente o mesmo conceito que determinada palavra de uma língua designa, em comparação com outra língua, e o dicionário oferece diversas expressões aparentadas que se aproximam do significado, só que não de modo concêntrico, mas em várias direções como na figura precedente, estabelecendo assim as fronteiras entre as quais esse significado se encontra.*

Desta maneira, devemos interpretar conforme o contexto contemporâneo da palavra, que vai além da simples Vigilância e se tornando o meio pelo qual governos e grandes corporações obtêm dados dos cidadãos.

Atualmente somos vítimas do controle exercido por estes entes, seja através de nossos computadores, celulares ou câmeras de segurança. Desde uma compra virtual, onde o vendedor salva os acessos dos seus compradores para direcionar a publicidade, ou um email enviado a um familiar, estamos sujeitos à Vigilância a todo o momento. Milhares são as maneiras pelas quais nossas ações são visualizadas e catalogadas.

Surveillance é a atenção sistematizada, rotineira e concentrada às informações de pessoas ou grupos que se deseja controlar, proteger e até influenciar. Sistematizada, pois essa atenção é deliberada e depende do uso de procedimentos específicos para ser alcançada. Rotineira porque faz parte do cotidiano de todas as sociedades atuais, seja no campo econômico ou estatal. Concentrada tendo em vista que seus alvos finais são os indivíduos.

O fato de a informação ser algo impalpável remove qualquer limite que poderia ser colocado, acabando assim com a fronteira entre público, privado, nacional ou internacional. Desta forma, diversas empresas começaram a produzir

tecnologias que permitem o controle e o reconhecimento individual, e diversos países começaram a utilizá-los.

Temos o exemplo emblemático do caso Snowden, um analista de segurança que trabalhava para uma empresa terceirizada da NSA – Agência Nacional de Segurança americana – que trouxe à tona a existência de dois sistemas de monitoramento: *PRISM* e *Upstream.* Estes sistemas permitiam ao governo norte-americano interceptar, armazenar e catalogar quase tudo que circula na Internet, além de todos os dados presentes nos servidores das grandes empresas de tecnologia da informação.

Posteriormente foi descoberta a existência de outro sistema, chamado de *Xkeyscore*, através do qual os funcionários da NSA conseguem analisar, sem mandado judicial, em tempo real e retroativamente, todas as atividades da Internet – e-mails, visitas a websites, conversas pessoais, pesquisas – de qualquer pessoa no mundo.

É um engano acreditar que essas sejam ideias novas. No passado, um dos casos mais famosos foi o do sistema *ECHELON*. Ele surgiu antes mesmo de 11 de setembro e da Guerra ao Terror. Tratava-se de um sistema de cooperação internacional entre Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia, capaz de interceptar qualquer transmissão de dados e voz via fibra ótica, cabos, satélites, rádio e micro-ondas. Sua existência foi negada por muito tempo antes de ser descoberta pela “Comissão Temporária Sobre o Sistema de Interceptação ECHELON” do parlamento europeu.

Não são apenas os governos que se utilizam deste tipo de instrumento para obter informações. Grandes companhias como Google, Facebook, Amazon, entre outras, utilizam informações obtidas por seus usuários para direcionar publicidade e desta forma obter lucro. Além disso, diversas das informações obtidas por essas empresas também são enviadas aos governos que passam a saber tudo sobre o cidadão – aonde ele vai, o que ele faz, com quem faz, o que ele compra, o que gosta e quem gosta. Tudo fica acessível, sem regras, e não sabemos o que é feito com estas informações.

Apesar de já ser mundialmente abordado pela sociologia, este tema ainda não é tratado com a devida importância pelos juristas brasileiros. Por ser de tamanha importância, eles não podem se eximir de sua responsabilidade com as garantias e direitos fundamentais dos cidadãos.

Recentemente foi aprovado pelo Congresso brasileiro o Marco Civil da Internet – Lei nº 12.965/14 -, que foi objeto de muitas discussões e negociações. Ela objetiva regulamentar o acesso a Internet no país, definindo princípios, garantias, direitos e deveres, nos termos do caput de seu artigo 1º. No entanto, devemos questionar se ele é capaz de proteger os indivíduos dos abusos do governo e das corporações transnacionais.

O fluxo de informação é extremamente volátil e desespacializado, portanto é inviável para o Direito, por estar associado aos conceitos de territorialidade e soberania, controlar o que é transmitido em nível global.

Embora seja um avanço reconhecido no mundo todo, o Marco Civil não é um meio hábil para impedir que estas práticas ocorram. A tentativa de regulamentar uma matéria abstrata, imaterial e dispersa mundialmente em um ambiente limitado é retrógrada e mostra que precisamos entender melhor essa dinâmica para que possamos trazer soluções concretas para o problema.

Além da promulgação desta lei, o governo adotou outras medidas, após a divulgação de que o governo norte-americano estava espionando membros do governo brasileiro[1]. Entre elas, estavam a realização de diversos debates diplomáticos e a criação de um sistema nacional de e-mail, que seria gerido pelos Correios. Esta última medida apenas demonstra mais uma vez o desconhecimento do governo sobre o tema, tendo em vista que este meio não teria sucesso nenhum em impedir a espionagem.

A problemática do Surveillance em nossa sociedade vai além do escopo garantidor do princípio do direito à privacidade. Hoje em dia, além do viés econômico por trás deste tipo de invasão, está também o argumento da segurança nacional. Assim, as informações não são simplesmente coletadas, mas processadas e

[1] http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html. Acesso em 20 de maio de 2015.

classificadas em categorias das quais desconhecemos a metodologia. Desta forma, não apenas a garantia à privacidade, mas o princípio da igualdade também é ferido, uma vez que as pessoas são categorizadas em grupos como “amigos” ou “inimigos”.

Assim, as desigualdades sociais são potencializadas, já que a retenção dessas informações permite a criação de grupos sociais arbitrários, que visam apenas à inclusão ou exclusão destes indivíduos. Em uma democracia, é inaceitável que as pessoas estejam sendo observadas e previamente julgadas, através de sistemas automatizados, por determinadas ações sem o direito a ampla defesa, o contraditório e o devido processo legal.

Tendo por base toda a problemática exposta, este trabalho tem por objetivo questionar a legitimidade e a legalidade das ações apresentadas – tanto dos governos quanto da iniciativa privada –, suas consequências e propor soluções no âmbito jurídico. Será abordado todo o histórico do conceito de Vigilância, os interesses estatais e econômicos por trás da prática, suas ofensas constitucionais e questionaremos as medidas tomadas pelo Brasil para tentar frear o controle exercido por esses poderes paralelos.

2. O CONCEITO DE SURVEILLANCE E UM BREVE HISTÓRICO

A melhor definição da palavra Surveillance, no contexto atual da palavra, vem do principal autor sobre o tema, David Lyon[2]:

> *Embora a palavra "surveillance" normalmente tenha conotações de clandestinidade ou investigações secretas em atividades individuais, também existem significados bem mais avançados que se referem à rotina e atividade diária. Com raiz no verbo francês "surveiller", que literalmente significa "observar", surveillance se refere aos processos nos quais apontamentos especiais são feitos sobre certos comportamentos humanos que vão bem além da curiosidade sem valor.*

Assim, compreende-se que a Surveillance vai muito além da simples Vigilância ou espionagem de um determinado indivíduo. Ela é o conjunto de diversas ações que podem levar a consequências boas ou ruins, conforme veremos mais a frente.

Voltando bastante ao passado, em 1791, o filósofo inglês Jeremy Bentham publicou um artigo em que propôs o conceito de uma cadeia mais humanizada (para a época): o Panóptico. Em resumo, trata-se de uma cadeia circular, em que todas as celas possuem uma janela para que entre luz; no meio da prisão haveria uma torre de guarda, com cortinas de modo que quem está dentro consegue ver todas as celas, mas é impossível ver o que ocorre dentro da torre. Desta maneira, mesmo que não haja guardas dentro da torre, os presos sempre

---

[2] LYON, David. Surveillance Studies: An Overview. Cambridge: Polity Press, 2007. p. 13-14. Traduzido livremente do inglês: "Although the word 'surveillance' often has connotations of surreptitious cloak-and-dagger or undercover investigations into individual activities, it also has some fairly straightforward meanings that refer to routine and everyday activity. Rooted in the French verb 'surveiller', literally to 'watch over', surveillance refers to processes in which special note is taken of certain human behaviours that go well beyond idle curiosity [...] So what is surveillance? For the sake of argument, we may start by saying that it is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction. Surveillance directs its attention in the end to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional or spontaneous; it is deliberate and depends on certain protocols and techniques. Beyond this, surveillance is routine; it occurs as a 'normal' part of everyday life in all societies that depend on bureaucratic administration and some kinds of information technology. Everyday surveillance is endemic to modern societies. It is one of those major social processes that actually constitute modernity as such."

pensariam que poderiam estar sendo vigiados, se sentindo obrigados a agir de maneira correta. Desta forma, como diz Foucault, o preso estaria sempre em um estado de consciente e permanente visibilidade que asseguraria o funcionamento automático do poder.

Além de estimular o pensamento filosófico sobre uma pena que ressocializasse o preso ao invés de apenas puni-lo, Bentham foi responsável por iniciar o conceito de Surveillance nos moldes que conhecemos hoje.

Foucault analisou, em *Vigiar e Punir*, a figura do panóptico e demonstrou que a sociedade moderna criou, nos séculos XVII e XVIII, o *momento das disciplinas* e o conceito de *sociedade disciplinar*. Este criava corpos submissos se valendo da vigilância nas prisões, escolas, quartéis, por meio da sujeição implantada nos indivíduos que se sabiam observados.

Segundo o filósofo, o panóptico foi a forma escolhida para "[...] assegurar uma vigilância que fosse ao mesmo tempo global e individualizante separando cuidadosamente os indivíduos que deviam ser vigiados." (FOUCAULT, 2004 a, p.216). Ele escreve também que o panóptico representava "Um olhar que vigia e que cada um, sentindo o peso sobre si, acabará por interiorizar, a ponto de observar a si mesmo; sendo assim, cada um exercerá esta vigilância sobre e contra si mesmo" (Idem, p. 218).

Logo após, Deleuze surge com uma teoria que ele chama de *sociedade de controle*. Na concepção deste pensador, a partir da segunda metade do século XX, a *sociedade disciplinar* deu lugar à *sociedade de controle.* As inovações tecnológicas advindas no pós-Segunda Guerra seriam uma nova maneira de exercer o poder na sociedade moderna.

A diferenciação entre estes conceitos surge quando o controle sai de uma esfera local – dentro das instituições abordadas por Foucault – para todas as esferas da vida social.

Na sociedade disciplinar, o poder exercido pelo Panóptico só se encontra presente dentro da instituição (escola, quartel, hospital) objetivando instaurar a disciplina e um padrão de comportamento. Já no modelo da sociedade de controle,

segundo Deleuze, o controle sai deste âmbito local e estende-se a todos os espaços da vida pública.

Com o avanço tecnológico e a criação de sistemas de câmeras se tornou possível monitorar não apenas os presos, mas toda a sociedade. O ideal de controle através do medo (de ser observado) de Bentham alcançou seu patamar mais alto neste momento.

Os circuitos fechados de televisão (CFTV) começaram a ser desenvolvidos ainda na década de 40 do século passado e passaram a ser implementados em ambientes públicos em 1973, na Times Square em Nova York.

Hoje em dia, os Estados Unidos e o Reino Unido possuem os maiores sistemas de CFTV no mundo.

Para se ter ideia, em 2013 o Reino Unido possuía cerca de 5.9 milhões de câmeras – uma para cada 11 cidadãos[3]. A rede de câmeras nas rodovias da Grã-Bretanha capturava automaticamente, através de um sistema de reconhecimento de placa, no início do ano passado, cerca de 26 milhões de imagens por dia, com informações do veículo, horário, data – ou seja, eles sabem para onde o cidadão foi, quando foi, quando voltou. Estima-se que o banco de dados tenha cerca de 17 bilhões de imagens em seu arquivo; o maior do tipo no mundo. A estimativa é que em 2018 sejam capturadas entre 50 e 75 milhões de imagens automaticamente por dia[4].

Em Chicago, nos EUA, há hoje pelo menos 22 mil câmeras instaladas, sendo uma das maiores redes do país. Sempre que alguém liga para o número de emergências o sistema identifica o local da ligação e mostra para o atendente uma imagem ao vivo da câmera mais próxima deste local[5].

[3] http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html. Acessado em 21 de maio de 2015.
[4] http://www.theguardian.com/uk-news/2014/jan/23/cctv-cameras-uk-roads-numberplate-recognition. Acessado em 21 de maio de 2015.
[5] http://www.wsj.com/articles/SB10001424052748704538404574539910412824756. Acessado em 21 de maio de 2015.

A indústria estima que o mercado de câmeras de segurança global vá crescer de US$13.98 bilhões em 2013 para US$42.06 bilhões em 2020[6].

No entanto, precisamos questionar a efetividade do uso deste tipo de sistema para diminuir a criminalidade. Uma análise publicada em 2008 pela Campbell Colaboration[7] evidenciou que o uso do circuito fechado de tem um efeito modesto na diminuição da criminalidade. Eles revisaram 44 estudos que usavam estatísticas para medir se o CFTV ajudava a diminuir a incidência de crimes.

A análise concluiu que o uso de circuitos fechados de televisão ajudaram a reduzir em 51% o roubo a veículos em estacionamentos e em 23% os roubos em transportes públicos. No entanto, em outros aspectos, ficou demonstrado que o uso de câmeras apresentou pequena ou nenhuma diminuição na taxa de criminalidade. Os próprios autores do estudo afirmaram que havia limitações nas informações utilizadas, por exemplo, se havia ou não placas que informassem a existência das câmeras – o que poderia influenciar na ocorrência do crime.

Em 2011 o porta-voz da cidade de Chicago, Jose Santiago, afirmou que o uso de circuitos fechados de TV ajudou a resolver, desde 2006, 4.500 crimes[8]. No entanto, estima-se que mais de um milhão de ocorrências tenham existido neste intervalo de tempo. Assim, conclui-se que menos de 1% dos crimes tiveram participação das câmeras em seu desfecho.

Outra forma de analisar a performance é quantos crimes cada câmera resolveu. Desta forma, conclui-se que apenas um crime foi solucionado para cada 5 câmeras, o que se mostra demasiado ineficiente.

É necessário mais estudo no tema, posto que não há muitas estatísticas disponíveis sobre a eficácia do uso deste meio para trazer segurança às grandes cidades.

Após décadas de crescimento no uso de CFTV, o advento e a popularização da Internet trouxeram novos meios para que o controle social ocorra.

---

[6] http://www.electronics.ca/store/video-surveillance-market-forecast-and-analysis.html. Acessado em 21 de maio de 2015.

[7] Welsh BP, Farrington DC. Effects of closed circuit television surveillance on crime. Campbell Systematic Reviews 2008:17 DOI: 10.4073/csr.2008.17.

[8] http://www.chicagobusiness.com/article/20110209/NEWS02/110209855/chicago-officials-defend-street-level-camera-network-as-money-saver-crime-fighter. Acessado em 21 de maio de 2015.

A capacidade de processamento dos computadores e o barateamento das tecnologias levou ao desenvolvimento de sistemas cada vez mais avançados na identificação e categorização automatizada de dados se tornaram os meios pelos quais hoje basicamente toda a informação é absorvida.

Bauman diz que a internet, nesta nova perspectiva, exerce a função de um *superpanóptico* (BAUMAN, 1999).

Esses *softwares* são capazes de filtrar os dados para encontrar pessoas ou mensagens de interesses. Os filtros são aplicados a celulares, computadores, circuitos de televisão e conseguem capturar voz, texto e imagens. Essas informações são processadas em grande velocidade e utilizadas para os mais diversos fins, que discutiremos mais a frente.

Além do poder público, grandes empresas de diversos ramos também se utilizam destes bancos de dados para os mais variados fins. Hábitos de compras, geolocalização dos celulares, pesquisas na Internet, tudo é absorvido por estas companhias para serem utilizadas com fins publicitários, criando uma versão virtual do ser humano – os *data-doubles*. Estas informações são coletadas com ou sem o consentimento do usuário, que permitem a o desenvolvimento de técnicas de classificação social das pessoas em categorias, o que pode gerar discriminação social e violação da igualdade.

Na década de 1940 os nazistas já utilizavam um sistema de processamento de dados (*Hollerith, da IBM*) para catalogar os judeus e outros grupos[9]. Edwin Black afirma que, se não fosse por este sistema, não seria possível ter ocorrido o Holocausto. Portanto, precisamos democratizar o uso dessa informação tendo em vista os preceitos fundamentais presentes em nossa constituição para que novos abusos não venham a ocorrer.

Não devemos supor, no entanto, que a mera criação de leis nacionais seja suficiente para proteger o cidadão destas invasões. Estes instrumentos são, por sua natureza, completamente insuficientes para resolver este problema.

Primeiramente, vamos entender as garantias feridas pelo fenômeno do Surveillance.

---

[9] BLACK, Edwin**. IBM e o Holocausto**. Rio de Janeiro: Campus, 2001.

3. DAS GARANTIAS LEGAIS E CONSTITUCIONAIS

Para se compreender inteiramente o fenômeno da Surveillance, precisamos analisar de forma analítica os aspectos jurídicos que estão vinculados ao tema.

Conforme descrito anteriormente, alguns princípios constitucionais são diretamente ofendidos, como o direito à privacidade (artigo 5º, inciso X, da Constituição Federal), o princípio da igualdade (este no *caput* do artigo 5º do mesmo diploma legal).

Ademais, devemos estudar também a maneira como o Marco Civil da Internet (Lei número 12.965/14) regula e fiscaliza possíveis abusos que possam vir a ocorrer na rede.

Por fim, será proposta uma nova abordagem para o uso do instituto do *Habeas Data*, baseada no seu conceito original e adaptada para a realidade em que vivemos.

Iremos agora esmiuçar cada um destes tópicos separadamente.

3.1 DO DIREITO À PRIVACIDADE

A nossa constituição garantiu o direito a vida privada como um direito fundamental, ou seja, faz parte de um conjunto de princípios básicos fundamentais à uma vida digna.

O direito à privacidade começou a ser mais amplamente discutido após um artigo publicado na *Harvard Law Review* em 1890, o “Ensaio Warren-Brandeis”. Escrito pelos advogados Samuel Warren e Louis Brandeis, o ensaio tinha o intuito de debater os excessos praticados pela imprensa norte-americana, que frequentemente expunha a vida das pessoas públicas. O artigo, que também ficou conhecido como “*The Right to Privacy*”, determinou a noção de “privacy” e do “right to be left alone” (o direito de estar sozinho) (LOPES, 2005).

Já naquela época, “invenções recentes” invadiam a privacidade das pessoas e estes autores perceberam a importância de se proteger quanto a isto:

> *Invenções recentes e métodos de negócio chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa, e para garantir ao indivíduo o “direito de ser deixado em paz”. Fotografias instantâneas e tablóides invadiram os recintos sagrados da vida privada e doméstica. Durante anos houve um sentimento de que a lei deveria dar solução para a circulação não autorizada de retratos de pessoas privadas e para a invasão de privacidade pelos jornais. [...] O princípio que tem sido aplicado para proteger estes direitos é, na realidade, não o princípio da propriedade privada. O princípio que protege escritos pessoais e quaisquer outras produções do intelecto ou emoções, é o direito à privacidade, e a lei não tem nenhum novo princípio para formular quando se estende essa proteção à aparência pessoal, palavras, atos, e de pessoal relação doméstica ou de outra forma.*[10]

Em 1948, a Declaração Universal dos Direitos Humanos já expunha a necessidade da proteção da vida privada e da intimidade nos termos de seu artigo 12, *in verbis:*

> *Artigo 12. Ninguém será sujeito à interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.*

A Convenção Europeia dos Direitos do Homem, em 1950, também definiu normas que garantiam o direito à privacidade e intimidade. O artigo 8º determina que “qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”. O mesmo artigo ainda reflete que não pode haver interferência estatal numa sociedade democrática, salvo se constituir na lei, para proteção, segurança, defesa da sociedade.

No Brasil, o direito à privacidade como direito personalíssimo e fundamental à dignidade da pessoa humana apenas foi reconhecido na Constituição de 1988, no inciso X do artigo 5º, como segue:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

[10] Tradução livre do conteúdo do ensaio, disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acessado em 21 de maio de 2015.

> *X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

Também no Código Civil de 2002 encontra-se um dispositivo legal com a finalidade de proteger a vida privada:

> *Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.*

Vida privada é um conceito variável, que muda conforme cultura, época e costumes de uma sociedade. À privacidade deve-se proteção, em relação ao Estado ou a particulares, que por algum determinado interesse podem “perfurar” a barreira entre o público e o íntimo do indivíduo (NASCIMENTO, 2009, p. 23-24).

Em 1953 surgiu uma teoria conhecida como Teoria das Esferas (ou Teoria dos Círculos Concêntricos da Vida Privada). O alemão Heinrich Hubmann propôs a divisão da privacidade em três círculos concêntricos: privacidade (esfera externa), segredo (esfera intermediária) e intimidade (esfera interna) (GOMES, 2008, p. 20).

Heinrich Henkel, em 1957, também criou um conceito tripartite de divisão da vida privada (em sentido amplo): a vida privada em sentido estrito (esfera externa), a intimidade (esfera intermediária) e o segredo (esfera interna). Este entendimento acabou se tornando majoritário no Brasil, por ter sido difundido por Paulo José da Costa Júnior (DI DIORI 2012, p. 2). Ilustrativamente tem-se o seguinte (Costa Jr. 1995):

A privacidade se encontra mais externamente, já que nesta camada as relações interpessoais são mais rasas. Esta esfera de privacidade é uma situação de convivência com outros indivíduos, excetuando-se terceiros que não possuem qualquer relação mais próxima.

É possível existir interesse público na vida privada, contanto que sejam relevantes para a sociedade. O acesso público é limitado, mas possível, contanto que haja interesse público, como a quebra de sigilos bancários e telefônicos por decisões judiciais.

A esfera da intimidade, mais interna que a privacidade, visa proteger as relações mais íntimas, onde há um sigilo maior e que não há a necessidade do conhecimento por outros. Diz-se que “a esfera íntima protege a pessoa inteiramente, ficando a mesma intocável aos olhos e ouvidos do público” (SZANIAWSKI, 2005, p. 357-358).

O simples fato de o indivíduo expor fatos íntimos a amigos não tira o caráter de intimidade da informação, modificando assim a esfera da mesma. O que ocorre é a aproximação de terceiros a um conhecimento concreto da intimidade ou da privacidade (GOMES, 2008 apud DELGADO, 2005, p.24-26).

Nesta camada estão protegidos o sigilo domiciliar, profissional e englobando dados mais restritos sobre o indivíduo. Dados estes que são apenas compartilhados com familiares e amigos mais próximos.

A diferença entre estas duas camadas está no número de pessoas que tem acesso à informação, conforme o jurista José Adércio Leite Sampaio (2006). Se um fato só é sabido pelo próprio e mais alguns poucos amigos, é um fato íntimo. Já um fato que ultrapassa estes limites, mas não é aberto ao público em geral, é um fato privado.

O segredo é a última e mais interna camada da privacidade (sentido amplo). Nela, encontram-se informações que geralmente não são compartilhadas com nenhum outro ser humano.

Percebe-se, portanto, que quanto mais interna é a camada, maior a ofensa à dignidade daquele indivíduo e maior o dano causado.

Esta classificação, apesar de não ser absoluta, ajuda a definir parâmetros objetivos para a solução de eventuais problemas jurisdicionais. Isso impede que o julgador tome decisões subjetivas para decidir sobre casos de invasão de privacidade, baseado em suas crenças morais pessoais.

3.2 DO PRINCÍPIO DA IGUALDADE

O princípio da Igualdade é discutido desde a Antiguidade, na Grécia, por grandes filósofos como Clístenes, o pai da democracia Ateniense. Naquela época, no entanto, o conceito de igualdade só era válido para quem era considerado cidadão. Ou seja: homem, filho de pai e mãe atenienses e maior de 20 anos. Neste caso, mulheres, estrangeiros, escravos e menores não eram considerados cidadãos e portanto não tinham voz ativa na *polis*.

Como a vida pública e política era algo de grande valor para os gregos, o homem só existia de forma plena enquanto fazia parte da comunidade política. Isso tornava os não-cidadãos inferiores socialmente àqueles que eram assim considerados.

Assim, o conceito de igualdade estava presente naquela sociedade, mas não como o conhecemos.

Apenas no ano de 1215, quando o rei inglês João Sem-Terra assinou a Magna Carta, é que começou a surgir um conceito de igualdade mais próximo ao que temos hoje.

Este documento trazia limites ao poder monárquico na Inglaterra, o que fez surgir a primeira monarquia constitucional. Devido a desentendimentos entre João, a Igreja e grandes barões ingleses, o rei foi obrigado a assinar este documento em que ele deveria renunciar a certos direitos e respeitar determinados procedimentos legais.

Isto por si só não garante a existência da igualdade, mas foi um primeiro passo no sentido de evitar possíveis abusos por parte do poder público.

Na Antiguidade e na Idade Média a sociedade girava em torno de uma consciência de coletividade, em que o indivíduo deveria abrir mão de seus interesses pessoais pelo bem coletivo.

Ao fim da Idade Média os homens foram se mudando para as cidades, o que fez ressurgir o comércio e impulsionou as grandes navegações. Isso fez surgir a independência do homem em relação ao coletivo e os valores individuais foram começando a crescer dentro das pessoas.

Com estes eventos, o feudalismo foi chegando ao fim e a Igreja começou a perder força, levando à Revolução Científica e o surgimento de um novo conceito de igualdade.

Na modernidade o sujeito é colocado em primeiro lugar, com sues características peculiares, para depois pensar a sociedade, que nada mais é que o conjunto de interesses destes indivíduos.

O comércio estava cada vez mais se intensificando, porém os burgueses tiveram dificuldades em expandi-los devido à grande quantidade de moedas e impostos existentes entre os diversos feudos e cidades. Isto levou à centralização do poder na figura do Rei e a criação dos Estados Nacionais.

Estes mesmos burgueses, com muito dinheiro para investir, estimularam o desenvolvimento cultural, científico, filosófico e artístico que ficou conhecido como o Renascimento.

O Renascimento trouxe uma nova forma de ver o mundo, com ênfase no Antropocentrismo e maior foco no homem e sua individualidade. Aliada à ele, a Revolução Científica quebrou diversos paradigmas e verdades universais foram comprovadas erradas, o que se refletiu na sociedade.

Durante o século XVII ainda ocorreu a Revolução Inglesa. As disputas entre os reis da dinastia Stuart e o Parlamento Inglês causaram grande descontentamento aos burgueses. Ao final desta revolução foi assinada a *Bill of Rights*, que garantiu os princípios fundamentais burgueses e a afirmação dos direitos individuais.

Este conceito de igualdade que começou a surgir e se consolidou com a Revolução Francesa e com a Revolução Americana foi a chamada igualdade formal.

A igualdade formal é aquela que se baseia na lei, ou seja, a lei afirma que os indivíduos devem ser tratados de maneira igual, portanto eles são iguais. Ela possui apenas força normativa, mas não traz de fato a igualdade para a sociedade.

Este conceito se limita à abstenção estatal, ou seja, o Estado não pode intervir para garantir privilégios à certa classe. Ela visa abolir regalias de determinadas categorias. Não é discutida a igualdade de condições na participação social, tendo em vista que os burgueses apenas visavam acabar com os benefícios da nobreza.

Quando se fala em igualdade formal, busca-se a igualdade perante a lei e o tratamento igualitário dos indivíduos, sem haver diferenciação por atributos pessoais aos destinatários da norma. A igualdade formal é produto do Estado de Direito, que é pautado na lei, sendo a lei igual para todos.

A igualdade formal teve como seu marco maior a *Declaração dos Direitos do Homem e do Cidadão* de 1789, que reafirmou a igualdade e os direitos individuais.

A Revolução Francesa e a Revolução Gloriosa na Inglaterra foram bem sucedidas em expandir os ideais burgueses pela Europa, o que levou à Revolução Industrial – juntamente a uma filosofia Liberal que era disseminada na época.

Como afirma MAGALHÃES (2000, p.44):

> *Esse individualismo dos séculos XVII e XVIII corporificado no Estado Liberal e a atitude de omissão do Estado diante dos problemas sociais e econômicos conduziu os homens a um capitalismo desumano e escravizador. O século XIX conheceu desajustamentos e misérias sociais que a Revolução Industrial agravou e que o Liberalismo deixou alastrar em proporções crescentes e incontroláveis.*

A rápida expansão burguesa e a procura por riqueza levou a Europa à uma corrida imperialista, que fez expandir no mundo inteiro o capitalismo industrial. Isso gerou uma grande exploração das pessoas que fez crescer demasiadamente a desigualdade social entre os burgueses e o resto da sociedade.

Essa corrida imperialista foi responsável por diversas guerras, entre elas a Primeira Guerra Mundial, que ocorreu de 1914 a 1918. A partir dessa guerra o capitalismo passou a ter um viés um pouco mais social, tendo como exemplo a Constituição Mexicana de 1917 e a Constituição de Weimer de 1919, na Alemanha. Estes diplomas traziam em si os conceitos de direitos sociais e a proposta de construção de uma nova sociedade.

No entanto, algumas décadas depois, o surgimento de Estados totalitários e fascistas causaram a perseguição de milhares de pessoas e uma grande repressão ao povo, principalmente às minorias.

Isso levou, ao final da Segunda Guerra Mundial, à criação das Nações Unidas. Por causa do grande abuso aos direitos humanos durante a guerra, foi expedida a Declaração Universal dos Direitos Humanos, que logo em seu primeiro artigo determina a igualdade entre todos.

Neste momento, o conceito de igualdade começa a mudar. A igualdade formal, meramente jurídica, passa a ser substituída pela igualdade material, que visa, na prática, conquistar o bem-estar social.

A partir disso, diversas medidas devem ser tomadas – como ações afirmativas – para que os indivíduos de uma sociedade sejam, de fato, iguais.

Como escreveu Ruy Barbosa em "Oração aos Moços", em 1920[11]:

> *A regra da igualdade não consiste senão em quinhoar desigual–mente aos desiguais, na medida em que se desigualam. Nesta desigualdade social, proporcionada à desigualdade natural, é que se acha a verdadeira lei da igualdade. O mais são desvarios da inveja, do orgulho, ou da loucura. Tratar com desigualdade a iguais, ou a desiguais com igualdade, seria desigualdade flagrante, e não igualdade real.*

Este famoso texto resume bem o ideal de igualdade material que visa procurar o bem-estar de todas as pessoas de uma comunidade, garantindo a eles uma igualdade de condições, além da mera igualdade escrita na lei.

---

11 http://www.casaruibarbosa.gov.br/dados/DOC/artigos/rui_barbosa/FCRB_RuiBarbosa_Oracao_aos_mocos.pdf. Acessado em 21 de maio de 2015.

Após décadas de ditaduras em diversos países durante a segunda metade do século XX, os anos 1990 trouxeram o Estado Democrático de Direito. Este modelo propiciou o aumento da participação popular e permitiu que o cidadão participasse efetivamente das decisões políticas.

> *No constitucionalismo social pressupõe-se a crença de que a arbitrariedade ou o abuso dos direitos fundamentais pode ser evitado mediante o aumento do poder político do Estado para melhor controle das relações baseadas nestes direitos. No Estado democrático de direito há o pressuposto de que as causas destes abusos situam-se nas desigualdades sociais geradas pelas condições econômicas, políticas e sociais. Uma política eficaz para evitar estas arbitrariedades exige transformações econômicas, políticas e sociais, através da participação dos cidadãos nos centros de poder e fortalecimento das instituições democráticas. (SOARES, 2004, p.219).*

No Brasil, a Constituição Federal, no *caput* de seu artigo 5º, prescreve que “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes [...]”.

Ainda na Constituição há outros dispositivos legais que visam objetivar a igualdade, tais como o artigo 3º, III, artigo 170, artigo 205, entre outros.

3.3 O MARCO CIVIL DA INTERNET

O Marco Civil da Internet – Lei nº 12.965/14 – foi aprovado em 2014, após cinco anos de discussões e debates no Congresso Brasileiro. Conhecido como “Constituição da Internet”, seu texto trata, dentre outras coisas, da privacidade dos usuários, a liberdade de expressão e da neutralidade da rede. Ele traz princípios, direitos e deveres para quem usa a Internet, assim como determina as formas de atuação do Estado.

Ele é considerado um texto pioneiro no mundo e foi escrito com a participação de milhares de pessoas através de um debate aberto por meio de um blog.

O Marco rompe com uma lógica de criminalização da Internet seguida por diversos países. Ao final dos anos 1990 e o início do século XXI, a restrição do uso da Internet era foco de grandes empresas, principalmente do ramo fonográfico, que

visavam defender sua propriedade intelectual. Em 1998 o Congresso americano aprovou o DMCA – *Digital Millenium Copyright Act* – que criminalizava não só a violação dos direitos autorais, mas também a criação e distribuição de tecnologias que permitissem burlar o *copyright.*

Já nos primeiros anos deste século, o temor de que a Internet fosse um território propício à disseminação de crimes, sua execução ou preparação, levou a um maior controle político da rede. Jacob Appelbaum, no livro *Cypherpunks*, publicado por Julian Assange com a colaboração de outros autores, denominou de "Os Quatro Cavaleiros do Infoapocalipse: pornografia infantil, terrorismo, lavagem de dinheiro e a guerra contra certas drogas" (Assange *et al*., p. 64).

Desta maneira, seria fundamental restringir as liberdades e ampliar a vigilância na Internet. Os Estados Unidos liderou uma pressão internacional para que governos criassem leis de controle na Internet.

A Convenção de Budapeste – ou Convenção Sobre o Cibercrime – é um tratado internacional de Direito Penal elaborado pelo Conselho da Europa sob pressão norte-americana. Ele foi apressado após os atentados de 11 de setembro e suas assinaturas começaram logo em 23 de novembro de 2001. Abordando temas como violações de direitos autorais, fraudes ligadas à computadores e pornografia infantil, ele entrou em vigor apenas em 2004.

Esta medida europeia estimulou o desenvolvimento deste tipo de lei ao redor do mundo. No Brasil, a Lei 84/99, conhecida como Lei Azeredo ou AI-5 Digital, já estava em discussão e ganhou força com a promulgação deste tratado. Ele ficou parado por cerca de 11 anos na Câmara dos Deputados até voltar à debate em 2010. Assim como a Convenção de Budapeste, esta lei visava criar punições e ampliar a vigilância no meio virtual. Como forma de impedir a aprovação deste texto, a sociedade se uniu e propôs o debate do Marco Civil da Internet, que veio a se tornar lei em 2014.

A regulamentação da rede ainda depende de um decreto presidencial que vai definir os termos que o Marco Civil deixou pendentes. Da mesma maneira participativa que a lei foi desenvolvida, este decreto também está sendo debatido

colaborativamente através da Internet. Qualquer pessoa, órgão, empresa ou instituição pode elaborar uma proposta de como deve ser o decreto regulamentador.

O Marco Civil da Internet envolveu uma série de debates e aborda diversos aspectos fundamentais do acesso à rede no Brasil. No entanto, para fins deste estudo, iremos apenas abordar o que concerne à privacidade e a liberdade de expressão, para não nos afastarmos demais do tema.

Apesar de ser um texto visionário e avançado no mundo, no que toca a garantia de direitos individuais na rede, algumas concessões tiveram que ser feitas para que a lei fosse aprovada no Congresso. Dentre elas, a guarda de *logs* se mostra como nociva à privacidade.

Log nada mais é que o registro de algum evento em um computador ou rede. O Marco Civil aborda três tipos de logs: Guarda de Registros de Conexão (artigo 13), Guarda de Registros de Acesso à Aplicações de Internet na Provisão de Conexão (artigo 14) e Guarda de Registros de Acesso a Aplicações na Internet na Provisão de Aplicações (artigo 15).

O artigo 5º define, no inciso VI, registro de conexão como o “conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”. Já o inciso VIII define registros de acesso a aplicações de internet como “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”.

Endereço IP (Internet Protocol) é o número que identifica cada aparelho conectado à Internet. Não existem dois IPs iguais na rede.

O artigo 13 determina que os provedores mantenham os registros de conexão, sob sigilo, pelo período de um ano. Estes dados podem ser importantes na resolução de crimes, ao ser possível localizar o IP que enviou os dados que causaram o crime, seja ele uma invasão a uma conta bancária ou a disseminação de fotos íntimas de outrem. Este dispositivo não é ofensivo à privacidade, pois as informações são sigilosas e só são acessíveis mediante ordem judicial.

O artigo 14 impede que os provedores guardem informações sobre a navegação dos usuários, sendo fundamental na garantia à privacidade. Como toda a informação acessada passa pela rede dos provedores, esta norma visa garantir que eles não possam armazenar os dados dos sites que visitamos – apenas são permitidos salvar a hora, data, duração e IP.

Por outro lado, o artigo 15 traz um grande problema à proteção na *web*. Ele obriga que os próprios sites armazenem os registros de acesso a aplicação dos usuários por seis meses. Isso permite que as empresas que detêm estes sites possuam diversos tipos de informação sobre o usuário, seus interesses e intimidades. Este dispositivo também viola os princípios constitucionais de presunção de inocência e da proporcionalidade.

A norma determina que os dados sejam registrados indiscriminadamente para o caso de ocorrer uma possível persecução criminal. No entanto, se não há presunção de culpa, não pode haver retenção de dados de maneira injustificada. O argumento da segurança não pode ser utilizado para se utilizar de medidas desproporcionais que tratem todos como suspeitos.

Atualmente, dados de navegação são extremamente valiosos. Empresas como o Google guardam há anos os dados de seus usuários e traçam seus perfis comportamentais, ideológicos e de consumo. Isso permite que ela venda estas informações para outras empresas que irão direcionar sua publicidade ou desenvolver novos produtos visando este mercado.

Iremos abordar este tema com mais ênfase a frente.

Ademais, após os seis meses que a lei prevê que os dados sejam "guardados sob sigilo, em ambiente controlado e de segurança", eles podem ser trocados com outras empresas. Esta informação pode ser processada e cruzada com outras de outros sites, o que seria uma imensa invasão da intimidade do indivíduo.

É importante que o decreto regulamentador da Lei 12.965/14 aborde este tema e proteja a privacidade dos interesses econômicos presentes na rede.

Acreditar que o uso de *logs* vá impedir – ou ao menos identificar o responsável deles – crimes na rede é uma ilusão. A maior parte dos grandes crimes virtuais – por grande estamos considerando pedofilia, fraudes, venda de ilícitos – ocorre utilizando métodos avançados que impedem a identificação do IP e a localização do criminoso.

Desta forma, mesmo que o Marco Civil seja um divisor de águas na regulamentação do ambiente virtual, reconhecido internacionalmente[12], ele ainda tem falhas. Falhas estas que podem vir a ser corrigidas com a edição do decreto presidencial que deve ocorrer ainda este ano. No entanto, é preciso que sociedade continue a pressionar, assim como pressionou durante a criação da lei, para que os direitos dos cidadãos sejam protegidos.

Tendo abordado os aspectos jurídicos que envolvem o tema, o trabalho continuará demonstrando de que forma estas noções interagem com a nossa realidade, nos aspectos governamentais e econômicos. Como o uso da Surveillance por estes atores afeta o indivíduo e sua esfera pessoal.

Além disso, vamos falar sobre como a sociedade respondeu à descoberta de alguns destes fatos – os casos de Edward Snowden e Julian Assange.

3.4. HABEAS DATA – UMA PROPOSTA

O *Habeas Data* é um instituto trazido pela Constituição de 1988 que visa garantir que o cidadão tenha conhecimento de informações a seu respeito que constem em registros de entidades governamentais ou que sejam públicos – e a retificação das mesmas. Conforme a nossa Carta Magna:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
>
> *LXXII - conceder-se-á habeas data:*

[12] http://webfoundation.org/2014/03/welcoming-brazils-marco-civil-a-world-first-digital-bill-of-rights/. Acessado em 21 de maio de 2015.

> *a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;*
>
> *b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;*

Durante a ditadura militar, com a criação do Serviço Nacional de Informações (SNI) em 13 de junho de 1964, foram catalogadas milhares de informações sobre os cidadãos que eram considerados subversivos.

Assim, o *Habeas Data* teve como influência duas décadas de investigação estatal na vida dos indivíduos, sem que se soubesse que tipo de informações o Estado tinha sobre eles. A constituição é clara quando diz que a informação tem que pertencer a uma instituição pública ou que, sendo de uma instituição privada, estes registros tem que ser públicos.

No entanto, devemos levar em consideração o contexto em que a norma foi elaborada. Nas décadas de 1980 e 1990 (quando a lei regulamentadora do instituto foi editada) o mundo era bem diferente de hoje. A presença da tecnologia nas nossas vidas cresceu de maneira absurda e hoje não existe um momento do dia em que estejamos afastados de algum aparelho conectado à Internet.

Conforme já foi falado e discutiremos mais a frente, esta presença tecnológica permitiu que empresas privadas também fossem capazes de armazenar dados sobre nós e, de diversas maneiras, utilizar estas informações para seus interesses próprios. Diferentemente do Estado, em que podemos eleger nossos representantes e propor leis que regulem a Vigilância, o caso das empresas se torna muito mais abusivo. Não há controle de que tipo de informação eles armazenam e o que vão fazer com ela. Os diretores da companhia determinam tudo, sem o consentimento do governo ou do povo.

Desta forma, como uma forma de proteger os direitos individuais, este trabalho vem propor que a aplicação do *Habeas Data* se estenda às informações possuídas por empresas privadas e que não sejam públicas.

Se o Estado tem o dever de prestar esclarecimentos sobre os registros individuais dos cidadãos, por que uma companhia privada pode manter seus bancos de dados em sigilo?

Como a própria lei do *Habeas Data* (Lei 9.507/97) determina, apenas o próprio interessado pode pedir informações sobre ele, então não haveria qualquer possibilidade de uso deste mecanismo por um terceiro para obter informações de outrem.

Este remédio constitucional tem como objeto protetivo os direitos da personalidade abrangidos pelo inciso X do artigo 5º da Constituição Federal – a intimidade, a vida privada, a honra e a imagem. Estas esferas personalíssimas tem ampla proteção jurídica em todas as áreas jurídicas: cível, penal e administrativa.

Para José Afonso da Silva[13], o *habeas data* tem como finalidade proteger a esfera íntima das pessoas contra:

> *[...] a) usos abusivos de registros de dados pessoais coletados por meios fraudulentos, desleais ou ilícitos; b) introdução nesses registros de dados sensíveis (assim chamados os de origem racial, opinião política, filosófica ou religiosa, filiação partidária e sindical, orientação sexual, etc.); c) conservação de dados falsos ou com fins diversos dos autorizados em lei.*

É fácil perceber que a iniciativa privada hoje tem plena capacidade de obter estes tipos de dados sobre os cidadãos. Nesta perspectiva, é preciso adaptar nossas ferramentas à realidade apresentada para que elas não acabem se tornando ineficazes ao que se propõe.

[13] SILVA, José Afonso da. **Curso de direito constitucional positivo**. 22.ed. rev. e atualiz. nos termos da Reforma Constitucional (até a Emenda Constitucional nº 39 de 19.12.2002). São Paulo: Malheiros, 2003. p.451.

4. SURVEILLANCE E O ESTADO

Nos dias de hoje não faltam motivos para o Estado justificar a invasão diária à privacidade dos indivíduos. Segurança pública, guerra ao terror, pedofilia, combate ao crime organizado, todos estes argumentos são utilizados para que o Estado limite os direitos individuais.

O cenário mais enfático deste uso é aquele do *Big Brother*, da obra "1984" de George Orwell. No texto de Orwell, um regime totalitário onipresente utiliza de meios avançados para fiscalizar a vida dos cidadãos, cerceando os direitos individuais.

Tirando do contexto este governo opressor (na maioria dos casos), não há muita diferença entre a realidade da obra e a nossa realidade. Os circuitos de televisão hoje são tal qual o olhar do Grande Irmão, que vê todos a todo o momento. A obra também aborda os conceitos de igualdade e dignidade.

Nos Estados Unidos, recentemente, ficou famosa a prática de Surveillance pela NSA (Agência Nacional de Segurança, do inglês). Diversos documentos vazados em 2013 por Edward Snowden, um funcionário de uma empresa terceirizada que prestava serviços para a Agência (e que iremos abordar em um capítulo mais a frente), demonstraram que o governo americano estava infiltrado na vida de milhares de cidadãos em pelo menos 193 países[14].

Este assédio cometido pelo governo estadunidense era validado, entre outras normas, pelo Patriot Act assinado pelo ex-presidente George W. Bush em 2001, e que chegou ao fim no dia 1 de junho deste ano. Este decreto permitia, entre outras medidas, que órgãos de segurança e de Inteligência interceptassem ligações telefônicas de pessoas ou organizações, estrangeiras ou americanas, supostamente envolvidas com terrorismo, sem a necessidade de ordem judicial e armazenar as informações por 5 anos.

[14] http://g1.globo.com/mundo/noticia/2013/07/as-principais-revelacoes-de-edward-snowden.html. Acessado em 21 de maio de 2015.

Um relatório da *World Wide Web Foundation* chamado de *Web Index*, publicado em 2014[15], mostrou que 84% dos 86 países pesquisados não apresentam leis ou as mesmas são insuficientes para impedir a vigilância em massa.

A ONU acatou, este ano, uma resolução proposta pelo Brasil criando um cargo na entidade que proteja a privacidade no mundo[16]. Este cargo teria o poder de monitorar a atuação dos serviços de Inteligência e governos para que se tenha um controle maior sobre a vigilância em massa na Internet. Governos de alguns países como Arábia Saudita, Emirados Árabes e África do Sul se opuseram à proposta, afirmando que não aceitariam a intromissão da entidade em seus países.

No ano passado, o Brasil também havia conseguido aprovar na Organização uma resolução que afirma que a espionagem em massa é uma violação dos Direitos Humanos. O Brasil assumiu este papel de protagonista na defesa da privacidade após a presidente Dilma Rousseff ter seu governo espionado por agências norte- americanas.

Em contrapartida, países como Holanda, África do Sul e Austrália seguiram no caminho oposto e aprovaram leis permitindo a obtenção de dados sem um mandado judicial. A França aprovou uma lei que permite a diversas agências verificar a conexão de usuários em tempo real sem a necessidade de um mandado judicial. No Reino Unido, a *Data Retention and Investigatory Powers Bill* (Lei de Retenção de Dados e Poder Investigativo, na tradução livre) foi aprovada rapidamente pelo Parlamento e aumenta o poder dos serviços de segurança.

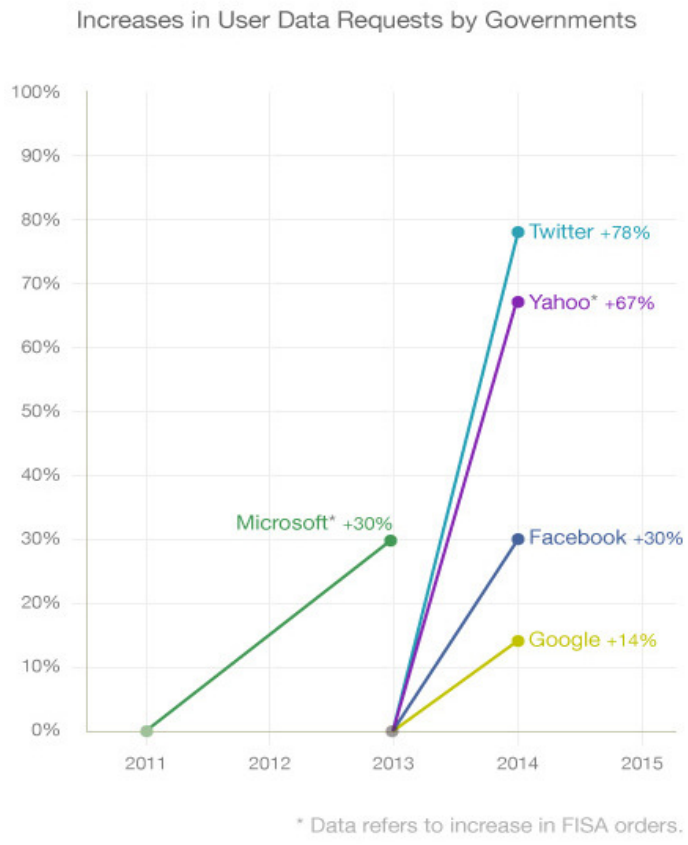
Uma pesquisa realizada pela Anistia Internacional com 15 mil pessoas em 13 países, publicada em março deste ano[17], mostra que 59% dos entrevistados é contra a vigilância em massa de seus próprios governos e que 71% são contra a espionagem dos Estados Unidos a outros países.

[15] http://thewebindex.org/. Acessado em 21 de maio de 2015.
[16] http://internacional.estadao.com.br/noticias/geral,onu-aprova-proposta-do-brasil-para-monitorar-direito-a-privacidade,1658398. Acessado em 21 de maio de 2015.
[17] https://anistia.org.br/noticias/pesquisa-inedita-indica-preocupacao-dos-internautas-brasileiros-com-vigilancia-e-privacidade-na-internet/. Acessado em 21 de maio de 2015.

Você acha que o governo [do seu país] deve ou não interceptar, armazenar e analisar o uso da internet e das comunicações de telefonia móvel ...

de todos os cidadãos vivendo no seu país.	Australia	Brasil	Reino Unido	Canadá	França	Alemanha	Holanda	Nova Zelândia	Filipinas	Africa do Sul	Espanha	Suíça	Estados Unidos
Sim, deve interceptar, armazenar e analisar o uso da internet e das comunicações móveis.	30	25	36	23	33	20	21	22	43	32	18	18	20
Não deve interceptar, armazenar e analisar o uso da internet e das comunicações móveis.	55	65	44	61	44	69	58	63	52	61	67	63	63
Sem opinião.	15	10	20	16	24	11	20	15	5	7	15	20	18

Além disso, entre 2013 e 2014 houve um aumento do número de informações requisitadas pelos governos às companhias que prestam serviços na Internet. O *Web Index* mostrou que empresas como Twitter, Facebook e Yahoo tiveram um aumento significativo nos dados prestados ao governo norte-americano, com base em um ato que permite a coleta destas informações (*US Foreign Intelligence Surveillance Act*)[18]:



Como já foi dito anteriormente, não é apenas a privacidade do cidadão que está em risco com estes abusos governamentais. A partir das informações

[18] http://thewebindex.org/report/#6.1_privacy_and_surveillance. Acessado em 21 de maio de 2015.

coletadas, o governo cria banco de dados e determina, de maneira que a sociedade não sabe, quem é bem-vindo e quem é inimigo do Estado.

Nas palavras de David Lyon (2003, p. 1)[19]:

> *Enquanto estes problemas ainda forem insignificantes, está ficando bastante claro para muitos que eles não nos contam a história toda. Pois a Surveillance hoje separa as pessoas em categorias definidas como dignas ou de risco, de forma que tem efeitos reais nas suas chances de vida. Discriminação profunda ocorre, tornando a Surveillance não apenas um problema de privacidade pessoal, mas de justiça social.*

Nesta seara, Didier Bigo (2008) utiliza o conceito de "ban-optique", que vem da junção de ban (no sentido de banimento) e optique, do panóptico de Bentham. Nesta nova realidade, o sentido do panóptico, que serve para disciplinar um grupo alvo, se inverte. O banóptico se volta para excluir da sociedade um grupo indesejado com o argumento de melhoria e segurança.

No mundo atual, podemos ver grupos estrangeiros e religiosos como alvo deste tipo de exclusão. Árabes e muçulmanos passam por um pente fino rigoroso ao tentar entrar nos Estados Unidos, mesmo sem qualquer prova de que tenham cometido qualquer tipo de crime durante sua vida, apenas por pertencer a estes grupos.

O que se vê é a utilização de um estado de exceção como regra de governo, já que constitucionalmente todos deveriam ser tratados de forma igual. Inverte-se a ordem e o sujeito é punido antes de realizar qualquer ação.

Assim, conjuntos de informações armazenadas e processadas são utilizadas para prever e prevenir condutas a partir da criação de perfis de risco. Estes perfis são montados automaticamente por supercomputadores programados, através de critérios desconhecidos, e determinam quem entra e quem é barrado em ambientes físicos ou virtuais.

A categorização não é uma coisa nova. No século passado também eram criados arquivos e fichas sobre as pessoas que serviam para classificá-las. No

[19] Traduzido livremente do original: "*while these issues are still significant, it is becoming increasingly clear to many that they do not tell the whole story. For surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice".*

entanto, naquela época, os dados eram arquivados fisicamente e não era tão fácil cruzar estas informações com outras. Além disso, eventualmente essa ficha era esquecida.

Hoje em dia, com a criação dos *data-doubles*, tudo sobre qualquer um que esteja em um ambiente eletrônico fica salvo perpetuamente na rede e a fluidez dos dados permite que essa informação seja utilizada por quem a possua.

Um caso exemplar é o do senador estadunidense Edward Kennedy, em 2004, que foi impedido de viajar por ter seu nome em uma lista de suspeitos de associação com o terrorismo. A simples presença de um nome em uma lista pode cercear direitos básicos de qualquer indivíduo.

Não há nenhuma divulgação sobre os critérios que definem a criação destas categorias, o que permite que um líder político possa, a seu bel-prazer, incluir ou excluir grupos e aumentar a desigualdade.

Ademais, a falta de transparência e publicidade na existência destes processos permite ainda um abuso de poder por aqueles que movimentam a máquina. Em agosto de 2013 a imprensa norte-americana divulgou informações em que se demonstrava que funcionários e terceirizados de empresas ligadas aos serviços de inteligência utilizavam estes mecanismos para espionar pessoas por motivos privados[20].

Os dados coletados pelos sistemas de vigilância eram acessados sem autorização e sem restrição pelos empregados, para invadir a privacidade de seus flertes, cônjuges ou pessoas com as quais tivessem qualquer tipo de interesse. Isso possibilitava chantagens, intimidações e perseguições que poderiam ser consideradas criminosas. Essa prática ficou conhecida como *LOVEINT* – junção de Love (amor, do inglês) com INT (prefixo de Inteligência).

Não podemos esquecer o problema dos CFTV, que já foi discutido anteriormente neste trabalho. Além de todas as informações pessoais existentes *online*, estes circuitos ainda permitem que se saiba quando o cidadão foi a algum lugar e o que ele fez.

[20] http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/. Acessado em 21 de maio de 2015.

Este conjunto de estratégias, juntamente com mecanismos de análise biométrica que ainda podem vir a ser implantados – como registro de íris, *scanner* facial, dentre outros – criam um potencial infinito de controle social, tal qual Orwell imaginou em sua obra. No entanto, como as pessoas colocam suas informações espontaneamente na rede, estas violações não geram revoltas como no livro. As pessoas não sentem sua privacidade invadida, ou sentem, mas aceitam como se fosse algo contra o que não se pudesse lutar.

Podemos ver que países considerados ícones democráticos, que garantem constitucionalmente os princípios fundamentais de dignidade humana, como a Inglaterra, Austrália, Holanda e Estados Unidos, parecem não aplicar estas normas no ambiente virtual.

No mundo "real", todos são iguais perante a lei e inocentes até que se prove o contrário. Por outro lado, na Internet todos são potenciais criminosos que se não forem vigiados irão roubar bancos e traficar.

Talvez por ser algo bastante novo ainda não seja muito bem entendido por políticos velhos. O ponto é que a Internet se tornou uma extensão da vida cotidiana e todas as garantias conquistadas nos últimos séculos devem ser respeitadas também neste ambiente. Aliás, não só os políticos devem assimilar isso, como a sociedade também precisa compreender que seus direitos não podem ser violados em prol de uma suposta promessa de segurança.

Estes meios já se provaram ineficientes para combater o terrorismo e outros crimes. Temos diversos exemplos, como os atentados ao metrô de Londres em 2005[21], à Noruega em 2011[22] e à Maratona de Boston em 2013[23], dentre diversos outros ao longo dos últimos 14 anos em que o uso do Surveillance se expandiu ao redor do mundo.

[21] www1.folha.uol.com.br/fsp/mundo/ft0807200501.htm. Acessado em 21 de maio de 2015.
[22] http://oglobo.globo.com/mundo/mat/2011/07/23/loiro-cristao-de-extrema-direita-anders-behring-breivik-estava-fora-do-radar-da-policia-norueguesa-924966408.asp#ixzz1T59WVJcO. Acessado em 21 de maio de 2015.
[23] http://noticias.terra.com.br/mundo/estados-unidos/atentado-na-maratona-de-boston-os-7-dias-em-que-os-eua-reviveram-o-terror,e223656dd933e310VgnVCM3000009acceb0aRCRD.html. Acessado em 21 de maio de 2015.

Inclusive, diversos especialistas apresentam estatísticas que demonstram, matematicamente, a ineficácia da prática[24]. Foi realizado um cálculo[25] supondo que o algoritmo da NSA para detectar comunicações tenha um percentual de acerto de 99% e, tendo em vista que existir um terrorista é algo raro em uma população – o autor estabeleceu um terrorista para cada milhão de pessoas (o que ele considera um número exagerado). Ele estimou ainda que este algoritmo seria bastante eficaz e apresentaria apenas um falso positivo para cada cem detecções. Com esta análise, o pesquisador estimou que apenas uma em cada dez mil comunicações interceptadas seria de um terrorista de fato.

Outros tipos de crimes também continuam ocorrendo em níveis inferiores da rede (como a *deep web*[26]), onde este tipo de controle não tem qualquer alcance ou ingerência.

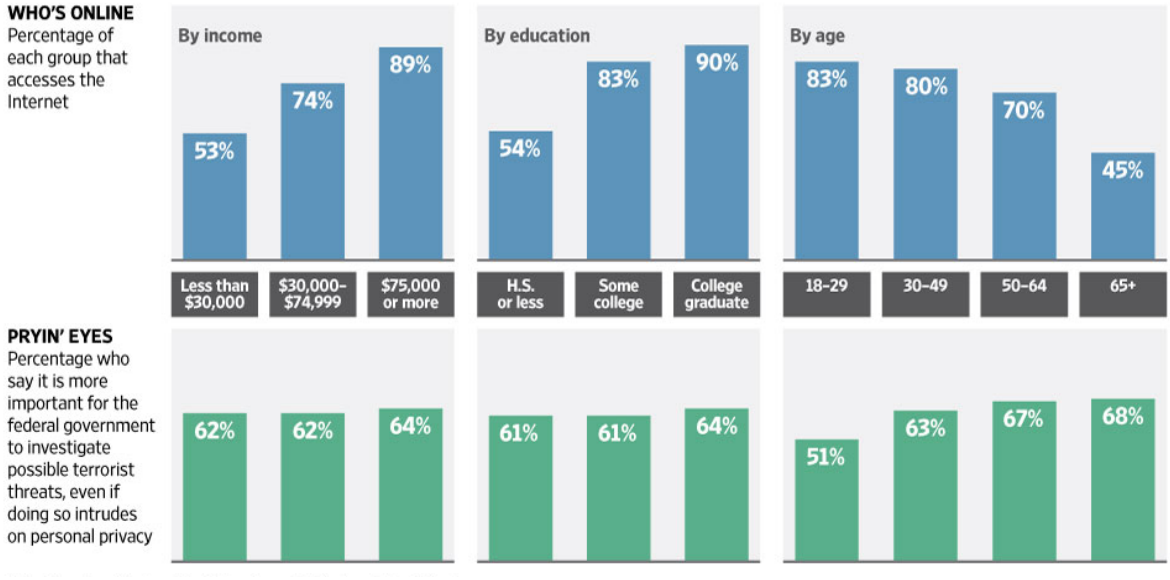
A pedofilia continua ocorrendo no mundo inteiro. Casos de discriminação contra grupos étnicos, sociais, religiosos, ou até mesmo contra nações inteiras seguem impunes na rede. A publicação de fotos e vídeos íntimos de terceiros ocorre diariamente, prejudicando a integridade de suas vítimas e mesmo com todo esse aparato não se conseguem alcançar os suspeitos. Roubos de informações bancárias, previdenciárias, entre outras, não conseguem ser coibidos.

Estas violações não podem ser aceitas como se fossem algo juridicamente legal. Mesmo que trouxesse qualquer tipo de resultado, o uso destes meios para atingir o fim a que se propõe ainda coloca os indivíduos na figura de suspeitos e viola uma série de princípios internacionalmente protegidos.

Uma pesquisa realizada em 2013 demonstrou que boa parte da população norte-americana concorda em abrir mão de seus direitos civis por uma maior segurança[27]. O estudo mostra que esse apoio é levemente maior entre grupos mais ricos e de maior educação, e que os jovens são aqueles com maior receio - apesar de mesmo assim haver bastante apoio à medida.

---

[24] http://www.wsj.com/articles/SB10001424127887324049504578543542258054884. Acessado em 21 de maio de 2015.
[25] http://bayesianbiologist.com/2013/06/06/how-likely-is-the-nsa-prism-program-to-catch-a-terrorist/. Acessado em 21 de maio de 2015.
[26] A deep web é uma parte da Internet criptografada e de acesso anônimo, requerendo programas específicos para acessá-la. As informações contidas nesta parte da Web não são indexadas pelos mecanismos de busca, ou seja, é impossível se pesquisar por qualquer conteúdo ali presente.
[27] http://www.wsj.com/news/interactive/POLCOUNT0614_pg. Acessado em 21 de maio de 2015.



Se fossemos trazer estes abusos virtuais para o mundo real, poderíamos imaginar um mundo onde seríamos revistados a cada esquina e que cada vez que saíssemos de casa para qualquer lugar deveríamos informar às autoridades. Qualquer coisa que se comprasse, qualquer jornal ou livro que fosse lido, tudo passaria pelas mãos do governo. As correspondências seriam lidas e toda conversa teria uma escuta.

Se esta realidade descrita gera revolta neste contexto, por que não acontece o mesmo no mundo virtual? Pois é exatamente isso que acontece diariamente, no mundo inteiro.

Com o fim do Ato Patriota, na noite do dia 31 de maio a NSA desligou seus computadores que analisam metadados. No entanto, o Congresso já discute uma nova lei, que está sendo chamada de *USA Freedom Act* – Ato de Liberdade. O que se propõe é que as companhias de telecomunicações armazenem as informações das pessoas, mas para que estes dados sejam analisados seria necessário um mandado judicial. No entanto, todas as investigações já iniciadas antes desta data ainda seguem as regras antigas.

Esta nova lei deve ser aprovada ainda este mês, e caso ocorra conforme se espera, haverá certo progresso no sentido do garantismo. No entanto, as empresas continuarão com acesso aos dados individuais e por si isso já é uma violação. Permitir que uma companhia privada armazene informações sensíveis sobre as pessoas abre uma série de questionamentos: qual a segurança protegeria

estas informações? Que tipo de treinamento os funcionários teriam para evitar possíveis abusos? Qual a legitimidade que a empresa tem para controlar desta maneira a vida dos indivíduos sem ordem judicial?

Tendo compreendido as questões debatidas neste tópico, vamos agora abordar como as corporações se valem desta realidade para seus interesses econômicos.

5. O USO ECONÔMICO DA SURVEILLANCE

Com o fim do modo de produção de massa fordista, e o início de uma cultura mais individualista, em que cada um passa a buscar uma experiência personalizada, o mercado se viu obrigado a procurar entender o que o consumidor buscava. O avanço tecnológico nos meios produtivos aumentou a produtividade e a eficiência da indústria e isso se refletiu na área do marketing, que visa estimular as pessoas a comprarem cada vez mais seus produtos.

As áreas de relacionamento com o cliente ganharam muita força. O *Customer Relationship Management* (Gestão de Relacionamento com o Cliente – CRM) é um grupo de mecanismos pelos quais se armazenam informações sobre o cliente para entregar produtos e serviços personalizados e aumentar a satisfação do mesmo. Um exemplo são os programas de fidelidade.

Atualmente este conceito evoluiu para o VRM – *Visitor Relationship Management*, em que as informações captadas do visitante de um site são utilizadas com algum fim econômico. Uma das primeiras empresas a se utilizar disto foi a Amazon, que de acordo com o histórico de buscas e compras dentro do site é capaz de fazer recomendações de outros produtos.

Um banco de dados que contenha o histórico de compras anteriores, dados pessoais (como idade, renda, data de aniversário), atividades, interesses, entre outras informações, é o sonho de qualquer setor de marketing de uma empresa.

A busca desenfreada pelo aumento de mercado consumidor fez com que as empresas também buscassem, através da Surveillance, meios de expandir sua área de alcance. Hoje em dia todas as grandes companhias – Google, Facebook, Amazon, Apple, Microsoft, Yahoo, Walmart, dentre muitas outras – criam *logs* de seus usuários que são utilizados para os mais diversos fins.

A questão não pode se limitar apenas à que tipo de informação elas possuem sobre nós, mas ao que elas podem fazer com isso, como vender ou transferir para outras iniciativas privadas ou governos.

Como Mark Andrejevic (ANDREJEVIC, 2009) exemplifica, imaginemos uma pessoa que decide pesquisar um problema médico na Internet. Enquanto a

informação médica de determinado indivíduo é considerada sigilosa, quando a pessoa faz uma pesquisa sobre aquilo na Internet, aquela informação é adicionada ao seu perfil virtual, juntamente com outras informações pessoais como relacionamentos, suas compras, seus interesses. A isso, Andrejevic chama de *digital enclosure* – ou invólucro digital – em que tudo sobre nós que está na rede é usado com um viés comercial.

Um exemplo prático do que foi descrito acima é o *Google Flu Trends*, um sistema do Google que coleta dados de pesquisas realizadas em seu site e, baseado em certos termos utilizados na pesquisa, consegue determinar e prever epidemias de gripe ao redor do mundo. Ele usa os endereços de IP salvos em seus registros para determinar de onde vem a pesquisa. Apesar disso, eles afirmam que a privacidade das pessoas está garantida pois os resultados são produzidos por um sistema automático[28].

Este método é conhecido como mineração de dados (*data mining*) e consiste em processar uma grande quantidade de dados em busca de padrões. Embora neste caso tenha uma finalidade positiva, pode ser usado para identificar necessidades, tendências, padrões e regras em grandes bancos de dados que podem gerar vantagens competitivas para aquela empresa.

Mantendo o foco no Google, vemos a utilização dessa técnica de maneira indiscriminada. Ela possui serviço de email, busca, redes sociais, venda de *banners* (principal meio de publicidade na Internet – é o *outdoor* eletrônico), entre outros. Eles processam a informação dos usuários adquirida através de suas trocas de email e utilizam estes dados para produzir propaganda de outras empresas que pagam por este serviço.

Por exemplo, um indivíduo troca emails com um parente afirmando querer viajar para um determinado país. Quase que imediatamente começam a surgir *banners* com pacotes de viagens, promoções e agências que prestam este tipo de serviço.

Qualquer informação que caia na rede – sejam compras na internet (ou a mera pesquisa por um produto), listas de amigos (que demonstram interesses em

[28] https://www.google.org/flutrends/about/faq.html. Acessado em 21 de maio de 2015.

comum), geolocalização de telefones celulares – é utilizada para traçar um perfil com a finalidade de aumentar o consumo. Hoje, simplesmente ao andarmos na rua, estamos passíveis a receber propaganda de algum serviço local em nossos celulares baseado no rastreamento de nossa posição e o envio desta notícia ao servidor.

Outro caso emblemático do uso abusivo de informações adquiridas sem consentimento foi um estudo secreto realizado pelo Facebook, juntamente com as universidades americanas de Cornell e da Califórnia[29]. O estudo, realizado em 2012, visava testar as emoções dos seus usuários e concluiu que aqueles que recebiam menos conteúdo negativo tinham menor propensão a também escrever conteúdos negativos. A pesquisa concluiu que "emoções expressadas por amigos, via redes sociais, influenciam nosso humor, constituindo, para nosso conhecimento, a primeira evidência experimental de contágio emocional de larga escala por meio de redes sociais".

Para isso, as informações recebidas pelos usuários foram manipuladas – sem um aceite prévio dos mesmos -, o que demonstra uma grande violação por parte da empresa. Isso serve para demonstrar o poder e o alcance que estes grupos econômicos têm em nossas vidas, baseadas em seus interesses e seus lucros.

A falta de consentimento dos usuários no uso de suas informações implica na violação de seu direito à privacidade. Mesmo que os usuários precisem concordar com os termos de uso de determinada página para poder usufruí-la (como no caso do Facebook), podemos equiparar estes a um contrato de adesão de prestação de serviços – já que o indivíduo não tem como debater as cláusulas presentes. Portanto, conforme o artigo 51, inciso IV e parágrafo 1º, inciso I, do Código de Defesa do Consumidor:

> *Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:*
>
> *[...]*
>
> *IV - estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade;*

[29] http://www.bbc.co.uk/portuguese/noticias/2014/06/140630_facebook_experimento_criticas_fl. Acessado em 21 de maio de 2015.

> *§ 1º Presume-se exagerada, entre outros casos, a vantagem que:*
>
> *I - ofende os princípios fundamentais do sistema jurídico a que pertence;*

Desta maneira, toda e qualquer cláusula que obrigue o cidadão a ceder seus dados para o livre uso pelas corporações é invalida tendo em vista que ferem princípios constitucionais – além de colocar as partes em patamares diferentes de igualdade na relação jurídica.

Além disso, o artigo 43 determina que os usuários, aqui equiparados a consumidores, tem o direito a saber tudo aquilo que é registrado sobre ele e deve ser informado por escrito sobre a abertura do cadastro:

> *Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.*
>
> *§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*
>
> *§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.*

Percebemos que estas regras não são seguidas pelos grupos que exercem seu mercado na *web*, o que mais uma vez coloca o indivíduo em uma posição de vulnerabilidade em relação às grandes corporações.

Trazendo de volta a discussão sobre o Marco Civil, em seu artigo 15, *caput*, fica determinado que:

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

Ao invés de proteger a informação pessoal do cidadão, este artigo não só permite como obriga as empresas a guardarem os dados de acesso de seus usuários, sem impor qualquer limite ao uso comercial dessas informações. O objetivo desta ordem legal é garantir a segurança na Internet (que conforme já foi

discutido, é insuficiente através destes meios), mas não foram definidas as regras que devem ser seguidas pelas companhias na posse destas informações.

Isso apenas legaliza uma prática já usual que deveria estar sendo coibida ao invés de fomentada.

Outro vácuo jurídico que esta norma deixa é o que deve ser feito com os dados após os seis meses que os provedores devem guardá-la. O texto apenas determina que a informação deve ser mantida sob sigilo durante este período, mas há uma brecha em relação ao uso dela posteriormente. Assim as companhias ficam livres para, depois deste intervalo, poder trocar, vender ou comprar bancos de dados gigantescos.

Como os custos para se manter uma estrutura que colete e mantenha em sigilo estes dados não são baixos, isto vai estimular o mercado de venda de metadados para compensar estes gastos. Empresas que não tinham o interesse na venda destas informações serão compelidas a fazê-lo ou podem ter prejuízos.

Ainda por cima, como existe uma ordem legal que manda que as empresas a guardem estes *logs*, não há mais a obrigatoriedade delas informarem que os registros estão sendo salvos.

Esta medida vai de encontro à decisão tomada pelo Tribunal de Justiça Europeu no ano passado, em que a Diretiva de Retenção de Dados de 2006 foi considerada inválida[30]. Diferentemente do Brasil, na Europa eram as empresas de telecomunicações que guardavam os registros de acesso. O Tribunal entendeu que:

> *"Estes dados, considerados no seu todo, são suscetíveis de fornecer indicações muito precisas sobre a vida privada das pessoas cujos dados são conservados, como os hábitos da vida cotidiana, locais de residência permanentes ou temporários, as deslocações diárias, atividades exercidas, relações sociais e meios sociais frequentados"*

O Tribunal considerou que a Diretiva atingia todos os cidadãos, meios de comunicação e dados de tráfego indiscriminadamente, e que não havia limites ou regras para o uso dos registros coletados.

[30]http://www.publico.pt/tecnologia/noticia/tribunal-de-justica-europeu-encontra-falhas-na-directiva-de-retencao-de-dados-1631459. Acessado em 21 de maio de 2015.

O Marco Civil ainda depende da edição de um decreto regulamentador a ser editado pela Presidente da República. Diversos grupos que lutam pela proteção dos direitos na Internet estão trabalhando para que sejam incluídos neste decreto normas que limitem o registro de dados e seu uso comercial pelas entidades privadas.

6. SOUSVEILLANCE – A VIGILÂNCIA INVERSA – E CONTRA-VIGILÂNCIA

No âmbito do estudo da Surveillance, não podemos deixar de abordar, ainda que de maneira breve, o crescimento da Sousveillance. Este termo foi cunhado por Steve Mann, um pesquisador de tecnologias captação de imagens, em seu artigo "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments" (Sousveillance: Inventando e Usando Aparelhos Vestíveis na Captação de Dados em Ambientes de Vigilância – tradução livre). Os prefixos "sur" (acima) e "sous" (abaixo), do francês, servem justamente para contrastar o ponto de vista de onde ocorre a vigilância.

Enquanto na Surveillance podemos utilizar a figura das câmeras de vigilância espalhadas por esquinas da cidade como aspecto básico do termo, na Sousveillance o foco vai para o indivíduo trazendo uma câmera ou outros meios de observação para o nível humano – seja no aspecto físico (uma pessoa carregando o dispositivo de fato) ou no aspecto hierárquico (pessoas comuns no controle desta esfera, ao invés de autoridades).

Neste viés surge a Surveillance Inversa, que nada mais é que o uso de gravações, monitoramentos e estudos dos sistemas de vigilância por aqueles que normalmente são alvos da Surveillance, para se proteger de abusos de autoridade.

Aqui no Brasil temos diversos exemplos que surgiram nas manifestações de junho de 2013, quando o uso de agressividade excessiva pela polícia foi exposto graças a vídeos gravados em aparelhos celulares. Uma mídia alternativa cresceu na Internet, produzida por pessoas que não eram do meio jornalístico, mostrando tudo aquilo que os grandes conglomerados de notícias, vinculados a interesses políticos e econômicos, não eram capazes de mostrar.

Um caso emblemático é o do estudante Bruno Ferreira Teles, que durante uma destas manifestações foi preso acusado de portar e lançar coquetéis molotov contra policiais[31]. Os principais meios de comunicação do país noticiaram a prisão alegando que ele era culpado, manchando a imagem do jovem. No entanto, imagens capturadas por um portal alternativo mostraram que na verdade foi um outro homem

[31] http://g1.globo.com/rio-de-janeiro/noticia/2013/07/inquerito-diz-que-manifestante-preso-no-rio-nao-portava-coquetel-molotov.html. Acessado em 21 de maio de 2015.

que lançou o artefato, suspeito de ser um policial infiltrado. As imagens divulgadas nas redes sociais foram suficientes para desmentir o que havia sido publicado e para que as denúncias contra o jovem fossem arquivadas.

A Primavera Árabe, uma onda de protestos no Oriente Médio e Norte da África que eclodiu em 2010, vem trazendo ao fim diversas ditaduras nessa região. O uso de redes sociais e ferramentas de *streaming* (transmissão ao vivo online) trouxeram grande visibilidade a estes eventos, muitas vezes contradizendo o que a grande mídia dizia e alçando altos níveis de audiência e compartilhamento.

Já na seara da contra-vigilância, também temos alguns casos emblemáticos. A contra-vigilância pode ser entendida como a exposição de informações sensíveis que o governo possui e que não pretende informar a população, apesar de seu dever de transparência.

6.1. WIKILEAKS

O maior ícone deste projeto na última década é o Wikileaks. Com sede na Suécia, o Wikileaks é uma ONG transnacional que publica de maneira anônima documentos, fotos e informações vazadas de empresas ou governos.

Seu principal ícone é o ciberativista Julian Assange, que ficou conhecido após o vazamento de milhares de documentos do governo americano sobre a guerra do Afeganistão. Estes arquivos comprovariam que o exército estadunidense cometeu diversos crimes de guerra, acobertados pelo governo[32]. Os relatórios abrangem o período de janeiro de 2004 até dezembro de 2009, e o Pentágono suspeita que o soldado Bradley Manning (Chelsea Manning atualmente) seja o responsável por vazar estas informações.

Além do Wikileaks, cinco outros grandes jornais ao redor do mundo também divulgaram estas informações: o espanhol *El País,* o alemão *Der Spiegel*, o francês *Le Monde*, o britânico *The Guardian* e o americano *The New York Times*.

[32] http://internacional.estadao.com.br/noticias/europa,wikileaks-diz-que-documentos-denunciam-crimes-de-guerra-no-afeganistao,586178. Acessado em 21 de maio de 2015.

Além destes documentos, diversos telegramas diplomáticos entre o governo dos Estados Unidos e suas embaixadas também foram vazados[33]. O escândalo ficou conhecido como *Cablegate*[34]. Foram mais de 251 mil documentos vazados de 274 consulados, embaixadas e missões diplomáticas ao redor do mundo.

Diversos deles tratam de maneira pejorativamente outros líderes mundiais e um documento, assinado pela Hillary Clinton, demonstrava técnicas de espionagem do governo norte-americano na ONU. O então Ministro de Relações Exteriores do Brasil, Celso Amorim, é descrito como um "oponente" [35] e o presidente do Afeganistão é considerado como tendo "uma visão de mundo paranoica" [36].

Estes e outros vazamentos acabaram gerando uma série de problemas para Julian Assange, que é procurado pelo governo americano. Após supostamente ter se envolvido em um escândalo sexual, ele foi convocado a prestar depoimento na Suécia. Temendo ir para lá, tendo em vista que a Suécia é parceira política dos Estados Unidos e poderia extradita-lo, ele pediu asilo à Embaixada do Equador no Reino Unido.

Assange é uma figura controversa e muitos afirmam que ele teria interesses ocultos com a revelação destes dados. Até agora, não temos como saber se há ou não qualquer interesse. No entanto, suas revelações foram importantes para expor a realidade que ocorre dentro de diversos governos.

6.2. EDWARD SNOWDEN E A NSA

Edward Joseph Snowden é um analista de sistemas que divulgou a existência de diversos sistemas, como o já citado *PRISM*, que compõe o programa de vigilância global da NSA juntamente com os *Cinco Olhos* (uma aliança de vigilância global composta pela Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos – aliança que surgiu com a já citada *ECHELON*).

[33] https://cablegatesearch.wikileaks.org/search.php. Acessado em 21 de maio de 2015.
[34] http://g1.globo.com/mundo/noticia/2011/09/wikileaks-publica-mais-250-mil-mensagens-diplomaticas-dos-eua.html. Acessado em 21 de maio de 2015.
[35] http://www1.folha.uol.com.br/poder/2010/11/838185-documentos-confidenciais-revelam-que-para-eua-itamaraty-e-adversario.shtml. Acessado em 21 de maio de 2015.
[36] http://www.bbc.com/news/world-us-canada-11862304. Acessado em 21 de maio de 2015.

Em uma entrevista em junho de 2013, Snowden revelou os motivos que o levaram a correr tamanho risco e divulgar as informações[37]:

> *"Eu sou apenas mais um cara que fica lá no dia a dia em um escritório, observa o que está acontecendo e diz: 'Isso é algo que não é para ser decidido por nós; o público precisa decidir se esses programas e políticas estão certos ou errados."*

Suas revelações são, em certa medida, fundamentais para que este trabalho esteja sendo elaborado.

Trabalhando como funcionário terceirizado da *Dell*, empresa que prestava serviços de TI (tecnologia da informação) para a Agência Nacional de Segurança, ele teve acesso aos computadores e a todo o tipo de informação ali existente. Ele então resolveu salvar estas informações em um CD e entregou aos jornalistas Glenn Greenwald e Laura Poitras em Hong Kong.

Alguns dias depois do vazamento, Snowden assumiu a autoria do roubo de dados e o Departamento de Justiça rapidamente o denunciou sob acusações de espionagem e roubo de propriedade do governo. Logo após, teve seu passaporte revogado.

O governo americano tentou extraditá-lo ainda na China, mas sem sucesso. De lá, Snowden tentou entrar na Rússia e foi impedido por não ter visto para ingressar no país. Com o passaporte cancelado, ele também não tinha como viajar para países na América do Sul que poderiam lhe dar asilo. Assim, ele permaneceu por 39 dias dentro do aeroporto enquanto solicitava asilo para diversos países, dentre eles o Brasil.

O Congresso brasileiro cogitou oferecer proteção diplomática para ele, tendo em vista as dezenas de invasões realizadas pelos americanos dentro do governo brasileiro que foram expostas pelo analista. Seria uma forma de demonstrar a indignação do Brasil aos abusos estadunidenses.

No entanto, pouco mais de um mês depois de ficar preso na zona de trânsito do aeroporto de Moscou, o governo russo garantiu a ele um asilo temporário de um ano. Quando este período se encerrou, a Rússia permitiu que ele residisse no país por três anos, podendo sair do país por não mais que três meses.

[37] https://www.freesnowden.is/frequently-asked-questions/. Acessado em 21 de maio de 2015.

Estima-se que ele tenha coletado mais de quinze mil documentos da Inteligência Australiana[38] e pelo menos cinquenta e oito mil da Inteligência Britânica[39]. Da NSA, inicialmente se acreditava que teriam sido roubados entre cinquenta mil a duzentos mil arquivos sigilosos. Posteriormente, no entanto, ficou constatado que foram baixados cerca de 1.7 milhões de arquivos da agência[40].

Os efeitos das revelações trazidas pelo Snowden são grandes e reverberam até hoje, dois anos após o ocorrido. Os dados apresentados trazem a tona uma realidade muito maior do que se imaginava no âmbito do controle social exercido por entes governamentais. Sempre se soube que o Estado utilizava de técnicas de escuta e espionagem para combater o crime, mas até então acreditava-se que para que isso acontecesse era necessário seguir um caminho legal e burocrático.

Snowden se arriscou para que os direitos fundamentais, garantidos pela constituição de seu país, fossem respeitados por aqueles que governam. É preciso que toda a sociedade compreenda a importância de seus direitos no ambiente eletrônico e que todas as lutas por direitos que ocorreram nos séculos anteriores terão sido em vão, já que a cada dia que passa tudo que acontece no mundo físico tem um reflexo no mundo virtual.

[38] http://www.theaustralian.com.au/national-affairs/foreign-affairs/edward-snowden-stole-up-to-20000-aussie-files/story-fn59nm2j-1226775491490. Acessado em 21 de maio de 2015.
[39] http://www.bbc.com/news/uk-23898580. Acessado em 21 de maio de 2015.
[40] http://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says. Acessado em 21 de maio de 2015.

7. CONCLUSÃO

Depois de uma análise profunda sobre o conceito de Surveillance, suas implicações, os métodos empregados, os interesses envolvidos na sua prática e as respostas sociais a esta atividade, podemos concluir que ainda falta um longo caminho a ser percorrido.

O panóptico, conforme concebido por Bentham e discutido por Orwell e Foucault em suas obras, alcançou um patamar que nenhum deles jamais imaginou e a Vigilância Global chegou ao seu ápice com os *smartphones*.

A regulamentação do tema ainda é precária no mundo inteiro, mas o Brasil vai dando seus passos neste caminho. Existem falhas a serem corrigidas na lei publicada, como o registro dos dados de usuários pelos provedores de sites, que ao invés de ser coibido, é obrigatório.

Bauman é bem incisivo quando diz (BAUMAN, 2001, p. 28):

> *A ausência de clareza das normas é o pior que pode acontecer às pessoas em sua luta para dar conta dos afazeres da vida. Uma vez que as tropas de regulamentação abandonam o campo de batalha, sobram apenas a dúvida e o medo.*

Ainda que o tema fosse regulamentado por muitos países, isso não garantiria o cumprimento das normas por empresas que prestam seus serviços além-mar.

O conceito tradicional de Estado Soberano é insuficiente para se discutir temas que possuem fluidez global. É questionável a eficácia do uso de regras locais na coibição deste tipo de prática. Embora por si só insuficiente para combater uma realidade em que os fluxos de dados se encontram desterritorializados, a produção de legislação é um caminho a se trilhar para começarmos o debate. Não se pode cobrar o que não está escrito.

Tratados internacionais devem ser discutidos, como os que o Brasil tem proposto na ONU, para que a comunidade internacional passe a respeitar não só os direitos de seus próprios cidadãos, mas do resto da população mundial – especialmente no caso dos Estados Unidos. (Mas não podemos nos limitar a ele.

Ele foi o que teve mais documentos vazados, mas práticas de outras nações podem existir sem que nós tenhamos o conhecimento).

As empresas devem ser mais transparentes com seus clientes e informar o que de fato pode ser feito com seus dados. Um contrato com letras pequenas que contêm abuso de direitos é inválido no mundo físico, então também não pode ser lícito no ambiente virtual. O consumidor desconhece as formas pelas quais é manipulado: o Google desde 2009 utiliza algoritmos que fazem com que cada pesquisa seja adaptada ao perfil do usuário – ou seja, os resultados das buscas não são neutros. Cada pessoa passa a ter uma experiência diferente ao usar o serviço, acreditando que é tratado da mesma maneira que todos os outros.

É preciso, acima de tudo, conscientizar a população global da relevância da defesa das garantias individuais, que foram produto de incontáveis lutas e séculos de progresso intelectual, desde a Magna Carta em 1215 com a limitação do poder monárquico na Inglaterra, passando pela Revolução Francesa com seus princípios de “liberdade, igualdade e fraternidade”, chegando ao século XX com a Declaração Universal dos Direitos Humanos, que foram o ápice da democracia moderna.

Parece que as pessoas acreditam que, por estarem em outro ambiente, não tem os mesmos direitos que tem na sua vida cotidiana.

Se um governo ditatorial começasse a registrar quem compra determinados livros, o reflexo seria de revolta e luta pelos direitos profanados. Mas pelo fato de nos encontrarmos sob uma ordem democrática e essa violação ocorrer de maneira passiva, sendo o próprio cidadão aquele que cede seus dados ao governo, ninguém parece dar a devida importância ao tema.

Este trabalho teve como objetivo colocar uma luz sobre um assunto ainda pouquíssimo discutido no âmbito jurídico brasileiro e, mais do que propor soluções, ele busca ampliar o debate das garantias fundamentais em um mundo fluido e imaterial.

Existe um universo muito maior dentro das redes de computação e dos circuitos de televisão. Universo este que a sociedade ainda desconhece, mas que faz parte de sua vida cotidiana. É preciso expor estes fatos e permitir que a

sociedade decida se concorda ou não com estas práticas. Cabe ao indivíduo, e não a qualquer governo ou empresa, determinar o que vale a pena se abrir mão para viver as “benesses” de um mundo informatizado, conectado e tecnológico. Qualquer coisa diferente disso é imposição e não condiz com os princípios democráticos que tanto valorizamos.

8. REFERÊNCIAS

ANDREJEVIC, Mark. *iSpy*: Surveillance and Power in the Interactive Era. Lawrence: University Press of Kansas, 2007. 325 p.

ASSANGE, Julian et al., *Cypherpunks* – Liberdade e o Futuro da Internet, São Paulo: Boitempo Editorial, 2013

BAUMAN, Zygmunt; LYON, David. *Liquid Surveillance*: A Conversation. Cambridge: Polity Press, 2012. 152 p.

BIGO, Didier. *Globalized (In) Security*: The field and the Ban-Opticon. In:_____; TSOUKALA, A. *Terror, Insecurity and Liberty*: iliberal practices of liberal regimes after 9/11. New York: Routledge, p. 10-48.

BLACK, Edwin**.** *IBM e o Holocausto*. Rio de Janeiro: Campus, 2001

COSTA JÚNIOR, Paulo José. "*O Direito de Estar Só*: Tutela Penal da Intimidade*"* 2ª Edição. São Paulo. Editora Rt, 1995.

DELEUZE, G. *Pourparlers*. Paris: Les Éditions de Minuit, 1990.

DI FIORE, Bruno Henrique. *Teoria dos círculos concêntricos da vida privada e suas repercussões na praxe jurídica*. 2012. Disponível em: Acesso em: 16 de abr. de 2014.

FOUCAULT, Michel. *Vigiar e punir*: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

HAGGERTY, Kevin D. *Tear down the walls*: on demolishing the panopticon.In: LYON, DAVID (org.). *Theorizing Surveillance*: The panopticon and beyond. Cullompton: Willan Publishing, 2006. p. 23-45.

LYON, David. *Surveillance Studies*: An Overview. Cambridge: Polity Press, 2007. p. 13-14

MAGALHÃES, José Luiz Quadros. *Direito Constitucional*. Tomo I. Belo Horizonte: Mandamentos, 2000. 414p.

MANN, Steve, NOLAN, Jason, WELLMAN, Barry. *Sousveillance*: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments.

ORWELL, George. *1984*. 29ª edição. São Paulo: Companhia Editora Nacional, 2003. 301 p.

SCHOPENHAUER, Arthur. *A arte de escrever*. Tradução de Pedro Süssekind. Porto Alegre: L&PM, 2009 176 p.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 22.ed. rev. e atualiz. nos termos da Reforma Constitucional (até a Emenda Constitucional nº 39 de 19.12.2002). São Paulo: Malheiros, 2003. p.451.

SOARES, Mário Lúcio Quintão. *Teoria do Estado*: introdução. 2. ed. Belo Horizonte: Del Rey, 2004. 404p.

SZANIAWSKI, Elimar. *Direitos de Personalidade e sua tutela*. São Paulo: Editora Revista dos Tribunais, 2005.

Welsh BP, Farrington DC. *Effects of closed circuit television surveillance on crime*. Campbell Systematic Reviews 2008:17 DOI: 10.4073/csr.2008.17.