Anais Eletrônico
IX EPCC – Encontro Internacional de Produção Científica UniCesumar
Nov. 2015, n. 9, p. 4-8
ISBN 978-85-8084-996-7

SOCIEDADE BIG BROTHER E OS LIMITES DA INTIMIDADE: A "VIGILÂNCIA LÍQUIDA" NA CONTEMPORANEIDADE.

Allan Bruno Gomes Ferreira[1], *Thomaz Jefferson Carvalho*[2], *Felipe Rangel da Silva*[3], *Luiz Felipe Rocha Caravelo*[4]

RESUMO: Este trabalho visa colocar em evidência o assunto da Vigilância Líquida e a Sociedade "Voyeurista ou big brother", não na conotação sexual da palavra, em *lato sensu* o termo refere-se ao excesso de curiosidade relacionada ao que é privado ou íntimo e a correlação destes atos na transgressão às leis no Brasil. Serão abordados temas que ao ser apresentado para a sociedade só evidenciam os pontos benéficos como: mais segurança, mais celeridade e mais conforto ao cidadão, não mencionando o ônus gerado e também como os dispositivos digitais são utilizados para violar direito fundamental como o direito à privacidade.

PALAVRAS-CHAVE: Cookies; Drones Civis; Sociedade Big Brother; Vigilância Líquida.

1 INTRODUÇÃO

É de fundamental importância observar as transformações que ocorrem na sociedade e ter atenção a necessidade de que direitos fundamentais e da personalidade não podem ser lesionados frente aos instrumentos tecnológicos que se apresentam cada dia mais inseridos na sociedade moderna.

Ao abordar o tema Vigilância Líquida e a Sociedade Big Brother, busca-se evidenciar como o fato da exposição das pessoas e de estarem constantemente sendo vigiadas e tendo seus dados coletados podem acarretar situações de desconforto e até mesmo de perigo real quando tais informações tem o propósito de atingir a honra, a incolumidade física ou obter algum tipo de vantagem indevida sobre o cidadão.

Será abordado também sobre os instrumentos, como os cookies, os Drones equipados com câmeras e outros meios empregados para que esta vigilância se torne possível, seja pelo Governo ou pelo seu vizinho, podendo refletir a partir desta análise acerca dos limites deste ostensivo controle.

E por fim, da necessidade de legislações específicas que disciplinem temas relacionados a dispositivos tecnológicos, dispondo sobre sanções aplicáveis caso haja lesão aos direitos dos cidadãos.

2 MATERIAL E MÉTODOS

Imbuído do conhecimento científico fez-se necessário um levantamento bibliográfico na doutrina nacional e internacional mais proeminente, bem como pesquisa documental na legislação vigente e análise jurisprudencial. Para tanto, utiliza-se como método no tratamento do conteúdo da pesquisa o dedutivo, histórico e tipológico para analisar o presente tema e desenvolver o presente estudo.

O foco principal é analisar na referência doutrinária a circunstância que acarreta essa sociedade ser denominada "Big Brother".

3 RESULTADOS E DISCUSSÕES

3.1 O Panóptico Digital

[1] Acadêmico do Curso de Direito do Centro Universitário Cesumar – UNICESUMAR, Maringá-PR. Estagiário da Carvalho & Rangel Advogados Associados. E-mail: allan@carvalhoerangel.adv.br e allanferreira.dir@gmail.com
[2] Mestre em Ciências Jurídicas pela UNICESUMAR; Pós-graduado *lato sensu* em Direito do Trabalho pela Universidade Castelo Branco e em Metodologia do Ensino Superior pela Universidade Norte do Paraná; Pós-graduando *lato sensu* em Ciências Penais pela Universidade Estadual de Maringá e Pós-graduando *lato sensu* em Direito Eletrônico pela UNESA - Universidade Estácio de Sá; Graduado em Direito pela Universidade Norte do Paraná. Advogado sócio da Carvalho & Rangel Advogados Associados. Presidente da Comissão de Direito Eletrônico e Crimes Virtuais da Ordem dos Advogados do Brasil, Subseção de Maringá, Seccional do Paraná, professor universitário no curso de Direito da UNICESUMAR, nas disciplinas de Direito Constitucional e Direito Empresarial II. E-mail: thomaz@carvalhoerangel.adv.br
[3] Pós-graduando *lato sensu* em Direito do Trabalho e Previdenciário pelo Instituto de Direito Constitucional e Cidadania, em convênio com a OAB/Maringá; Pós-graduado *lato sensu* em Direito e Processo Civil pelo Instituto Paranaense de Ensino em Maringá; Graduado em Direito pela Faculdade Maringá. Tem experiência em Direito Civil, Eletrônico e Administrativo, tendo atuado em escritório de advocacia na cidade de São Paulo e na Procuradoria Geral do Município de Maringá. Atualmente é vice-presidente da Comissão de Direito Eletrônico e Crimes Virtuais da Ordem dos Advogados do Brasil, Subseção de Maringá, Seccional do Paraná. Advogado sócio da Carvalho & Rangel Advogados Associados, responsável pelas áreas de Direito Civil e Direito Administrativo. E-mail: felipe@carvalhoerangel.adv.br
[4] Acadêmico do Curso de Direito do Centro Universitário Cesumar – UNICESUMAR, Maringá-PR. Estagiário da Carvalho & Rangel Advogados Associados. E-mail: luiz@carvalhoerangel.adv.br

A sociedade moderna encontra-se na era da tecnologia e a palavra que a descreve é Integração, ou seja, a necessidade de reunir, de aproximar países, culturas, compartilhar informações e até de solucionar situações políticas através de uma comunicação mais efetiva e célere, reflexo do fenômeno globalização que também perpassa em relação a informação.

Ao falar em sociedade moderna, a característica marcante que acomete essa modernidade é o fato de que esta não fica estática, é dizer, tudo muda muito rápido, o que hoje parece ser sólido no dia seguinte se desfaz, é o que o sociólogo polonês Zygmunt Bauman chama de "modernidade líquida".

Da mesma forma que não há como falar de "modernidade líquida" sem citar Bauman, não há como falar de vigilância sem destacar o modelo Panóptico desenhado pelo filósofo Jeremy Bentham, ao detalhar um projeto arquitetônico de vigilância, que permitia a um vigilante observar todos os prisioneiros sem que estes possam saber se estão ou não sendo observados. O francês Michel Foucault em sua obra Vigiar e Punir, destaca como a ideia de vigilância do panóptico de Bentham extrapolou a esfera da vigilância penitenciária para a qual foi criada, e passou a iniciar um processo de propagação ordenada de dispositivos disciplinares permitindo uma vigilância e um controle social cada vez mais efetivo.

Ao falar em controle social, é indispensável citar George Orwell que traz em sua obra distópica "1984", uma sociedade completamente vigiada e controlada por um Governo (no livro chamado de Partido) que tinha como o líder a figura do Grande Irmão (Big Brother) que adotava como seu slogan a expressão "O Grande Irmão está de olho em você", nesta ficção, o "Partido" utilizava-se de Tele Telas (uma espécie de televisão com câmeras) instaladas tanto em espaço público quanto no interior das residências para efetuar a vigilância destes cidadãos, onde estes em hipótese alguma poderiam manifestar pensamentos, opiniões ou qualquer outro ato que fosse contrário ou difamatório ao "Partido", sob pena de evaporar (sumir sem deixar rastros).

Ao relacionar a obra de Orwell com a ideia de Panóptico trazida por Foucault, percebemos que passamos da ficção distópica da obra "1984" para a realidade vivenciada na pós modernidade, é imperceptível mas não inexistente o controle e a vigilância da sociedade com os moldes do Panóptico, não com sua imensa torre de vigilância ao meio e envolto pelas celas prisionais com grandes janelas, mas sim, hoje representadas e internalizadas de forma discreta, dentro dos computadores, smartphones, câmeras de segurança e nos mais diversos aparatos tecnológicos.

Após o advento da criação e popularização da internet a fluidez trazida por Bauman se vê mais evidente, ao considerar que em um período curto de tempo passa-se da era analógica para ingressar na era da informação digital, representado por computadores cada vez mais rápidos e "inteligentes" que gerenciam vidas, por câmeras que dão sensação de segurança e smartphones com aplicativos com a função de informar até mesmo a hora de tomar água. Afinal, que nunca se sentiu "nu" ao sair de casa e esquecer o celular?

A sociedade assim como a tecnologia mudam cada vez mais rápido de forma espantosa, sendo quase impossível acompanhar a tecnologia que traz inovações a cada dia, são impressoras 3D com capacidade de criar órgãos humanos funcionais, drones capaz de auxiliar no combate de endemias e epidemias, inteligência artificial, redes sociais que integralizam desde comunicação instantânea e marketing de sua empresa a jogos on-line, mas será que isso não tem um preço além do preço pecuniário? Será que por traz do "Cadastro Gratuito, informe seu e-mail" não existem outras intenções por aqueles que irão receber seus dados?

Diante destas e de várias outras indagações é que se faz necessário que novas tecnologias que aparentemente foram criadas para auxiliar na segurança, na saúde e até mesmo para facilitar a vida dos cidadãos, devem ser observadas com "lentes" críticas e ser regulamentadas, impondo limites para que seu uso não venha a vilipendiar direitos basilares e inerentes ao ser humano.

3.2. Drones civis e a necessidade de legislação específica

Antes de desenvolver o assunto, é importante ficar atento a conceituação de drone adotado pela Anac, para a Agencia Nacional de Aviação Civil, drone é apenas um nome popular genérico, são utilizadas classificações técnicas como VANT (Veículo aéreo Não Tripulado), isto é, aeronave projetada para operar sem piloto a bordo de caráter não recreativo, como subcategoria tem-se o RPA (Remotely-Piloted Aircraft, em português, Aeronave Remotamente Pilotada), onde o piloto não está a bordo mas controla a aeronave remotamente se valendo de um dispositivo (controle, computadores, simuladores, etc.), sendo portanto a terminologia correta para referir-se aos drones[5].

Estas máquinas foram criadas inicialmente com fins militares, projetadas para serem empregadas em missões que oferecessem risco extremo aos militares, mas assim como a internet em seu início foi criada para os militares e acabou se popularizando os drones também chegaram ao meio civil, possibilitando hoje que qualquer cidadão possa adquirir um drone sem maiores fiscalizações ou requisito impeditivo.

[5] Conceituação retirada do link: http://www.brasil.gov.br/defesa-e-seguranca/2015/03/forca-aerea-esclarece-normas-para-voos-de-drones-no-brasil

Nov. 2015, n. 9, p. 4-8
ISBN 978-85-8084-996-7

O uso civil destas máquinas tem inúmeras aplicações que vão desde a produção de imagens por fotógrafos de casamentos até a utilização em resgastes de locais de difícil acesso, só que mesmo sendo perceptível a utilidade social deste equipamento se faz necessário a normatização e limitação do uso do mesmo, pois além de serem empregados para o bem social, por não ter requisitos impeditivos para a compra do aparelho, são também utilizados para violar direitos constitucionais como o direito à privacidade, a propriedade, a honra e a imagem.

Os drones podem ser facilmente "desviados" de suas funções aparentemente lícitas, como um simples voo em um local público ao passar ao lado de um edifício residencial e filmar no 10º andar uma pessoa nua na intimidade do seu lar; ou ao usar este drone para facilitar a vigilância da rotina de uma pessoa a qual se pretende sequestrar, tudo isso sem se expor, feito a distância, remotamente de um local que não pudesse ser identificado pelas vítimas ou policiais.

A ANAC (Agência Nacional de Aviação Civil), se atentando para o fato já se manifestou e propôs através da AIC N 21/10 – Veículos Aéreos Não Tripulados[6] e da Instrução Suplementar 21-002 Revisão A, intitulada "Emissão de Certificado de Autorização de Voo Experimental para Veículos Aéreos Não Tripulados"[7], algumas limitações para o uso destas máquinas, não é uma legislação específica ainda, mas sim um instrumento regulatório que dá os primeiros passos para a confecção de Lei própria.

A Instrução Suplementar da ANAC, orienta em pontos como a proibição de sobrevoar pessoas "inadvertidas" como em manifestações assim como os bens destas sem prévia autorização como imóveis e carros, sendo que para sobrevoar local público devem ter uma autorização da prefeitura e que devem conter placas informativas da presença de drones naquele local. Quanto aos espaços privados, como casamentos e festas, os drones de filmagens só poderão operar mediante prévia autorização de todos os presentes.

Alguns municípios brasileiros têm recrutado os drones no combate de epidemias e endemias, como no caso da Dengue, onde os veículos não tripulados são utilizados para transpor a altitude dos muros residências (ou não residências) com o intuito de detectar locais com possíveis focos de e reprodução e proliferação do vetor da Dengue.

Municípios como Maringá-PR que através do projeto de lei complementar que alterou a Lei Complementar 657/2007 que estabelece normas para evitar a proliferação dos vetores transmissores da Dengue, traz a proposta de inclusão de uso dos drones nas patrulhas de telhados, terrenos e outros locais de possíveis focos de procriação do vetor *Aedes Aegypty* , mesmo sem autorização do dono do imóvel sob o argumento de que poderão ser feita imagens para que posteriormente os agentes de saúde entrem em contato com o dono do imóvel ou até em caso mais extremo que sirva para que juízes defiram autorizações para a entrada nos locais.

Aparentemente a utilização desses métodos só trazem benefícios sociais, mas como levar em consideração a violação de um bem jurídico para proteger outro? Violar direito constitucional da propriedade, da privacidade para proteger a saúde da comunidade baseadas na suposição e desconfiança de que por um muro alto não permitir a visão, será utilizado um drone para a função. E se nada for encontrado, nenhum foco, se aquele cidadão tem a consciência de cuidar do seu espaço privado não permitindo que aquele local se torne um criadouro do vetor, como ficaria o seu direito constitucional que por "mera conduta" já fora usurpado?

São questionamentos pertinentes que devem ser levados em consideração e que necessitam o quanto antes de tutela jurídica, pois quando se fala da utilização destes meios tecnológicos visando diferentes finalidades, seja no emprego à área da saúde, da agricultura ou simplesmente utilizados como passatempo e diversão, esta tecnologia tem poder de vigilância e pode se tornar um instrumento em potencial seja contra o *Aedes Aegypty* ou contra o cidadão.

3.3. Sorria, os seus dados estão sendo coletados

A tecnologia ao evoluir busca formas de facilitar e agilizar a vida das pessoas, ao acessar a internet por exemplo, de forma automática abrimos o *browser* (em português, navegador) que permite o cidadão literalmente navegar em um "oceano" de informações. Devido à grande quantidade de informações disponíveis na internet e muitas vezes difíceis de encontrar um conteúdo especifico é que os famosos buscadores (google, yahoo, bing...) foram criados, visando a agilidade e a acessibilidade ao usuário comum.

Entretanto, nem tudo são flores, estes mesmos programas, aplicativos e aparelhos tecnológicos que entram na vida das pessoas para facilitar suas tarefas diárias, também estão sendo utilizados para violar a privacidade, através de coleta, armazenamento e redistribuição de dados pessoais sem ciência ou autorização dos legitimados.

Casos de espionagem empresarial, governamental e até de particulares são cada vez mais frequente pela facilidade que se tem acesso a informações como o nome da pessoa e seus familiares, seu endereço, telefone, e-mail e os sistemas de check-in dos aplicativos que amiúde informam sua localização.

[6] Departamento de Controle do Espaço Aéreo: http://publicacoes.decea.gov.br/?i=publicacao&id=3499
[7] Agência Nacional de Aviação Civil: http://www2.anac.gov.br/rpas/

Tais práticas são possíveis utilizando técnicas e mecanismos que na maioria dos casos é de desconhecimento da grande parcela de usuários comuns, como a utilização de Cookies ao acessar um site, sistemas de localização por GPS utilizado em smartphones e até mesmo o sinalizador de bateria do seu notebook.

Quando se fala em coleta de dados por sites e redes sociais o "Cookie" é a prática mais empregada entre outras inúmeras possibilidades. Para melhor esclarecer pode-se extrair um breve conceito sobre o que é "Cookies" do site da Microsoft[8]:

> Cookies são pequenos arquivos que os sites colocam no disco rígido do seu computador quando você os visita pela primeira vez.
>
> Pense em um cookie como um cartão de identificação que é exclusivamente seu. A função do cookie é notificar o site quando você voltar. Embora seja possível sua utilização indevida quando armazenam dados pessoais, os cookies em si não são Mal-intencionados. [...] Os cookies permitem guardar preferências e nomes de usuário, registrar produtos e serviços e ainda personalizar páginas.

Como já supramencionado, os "Cookies" podem ser utilizado de forma indevida pelos sites e redes sociais, o que de forma assustadora é mais comum do que se possa imaginar, é com base nesses "Cookies" que o Facebook foi acusado da prática de Stalking (em português seria o equivalente a espreitar / vigiar), a denúncia apresentada pela ACLU (União das Liberdades Civis Americana) ao Federal Trade Commission (Comissão Federal do Comércio) afirma terminantemente que: " The Social Network is Stalking You" (A rede social está seguindo você) e explica como acontece a vigilância[9]:

> "Quando você visita qualquer página no Facebook, ele instala Cookies em seu navegador, independentemente de você ter uma conta do Facebook ou de estar logado. Esses cookies alertam o Facebook cada vez que você visita um site que tem um botão "Like" ou que tenham outros plug-ins sociais do Facebook.
>
> Dado número de sites que usam o botão "Like" e outros plugins sociais do Facebook, dão ao Facebook a capacidade de rastrear uma enorme quantidade de seus hábitos de navegação. Eles sabem o que você lê, que vídeos você assisti, o que você compra, quem são seus amigos e qualquer outra coisa que você faz online.
>
> Mesmo que você saiba que este acompanhamento está acontecendo, você não tem acesso à informação que está sendo compilado sobre você, nem dão a oportunidade de corrigir eventuais erros ou esclarecer ou excluir qualquer coisa enganosa ou apenas embaraçosa. E enquanto o Facebook afirma que mantém essas informações apenas para melhorar a eficácia dos seus plugins sociais, perfis como o seu são uma mina de ouro em potencial para anunciantes on-line".

O Canvas Fingerprinting é outra ferramenta sorrateira alternativa aos já conhecidos "Cookies", que permite a vigilância de forma capciosa e é utilizada desde sites como o da Casa Branca dos EUA aos sites pornográficos, com a finalidade de manter o controle de quem os acessa.

O estudo sobre esta ferramenta, intitulado The Web Never Forgets (em português, A Internet nunca se esquece) e realizado por pesquisadores da Universidade de Princeton, explica melhor o que é esse API Canvas e como age este instrumento de vigilância[10]:

> Os autores descobriram que usando a API Canvas de navegadores modernos, pode-se explorar as diferenças sutis para extrair uma impressão digital consistente que pode ser facilmente obtido numa fracção de segundo, sem o conhecimento do utilizador.

Explicando melhor, esse API instrui os browsers (navegadores) a gerar de forma secreta uma imagem de sua máquina, como se fosse uma "impressão digital", onde através dessa imagem única (que irá seguir esta máquina para sempre), os sites atribuem a esta imagem uma numeração e a partir daí começam a coletar os

[8] Conceito retirado do Site Microsoft, no link: https://www.microsoft.com/pt-br/security/resources/cookie-whatis.aspx
[9] Tradução livre, informações extraídas do site: https://www.aclu.org/blog/speakeasy/social-network-stalking-you?redirect=blog/technology-and-liberty/social-network-stalking-you
[10] Tradução livre, informações extraídas do site: https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html#data

dados e traçar o perfil do usuário daquela máquina, direcionando melhor os anúncios que serão mostrados para ele. O site norte americano Pro Publica[11], traz as seguintes informações:

> Como outras ferramentas de monitoramento, as impressões digitais são usadas para construir perfis de usuários com base nos sites que visitam - perfis que formam os anúncios, artigos de notícias, ou outros tipos de conteúdo que serão exibidos para eles.
>
> Mas as impressões digitais são extraordinariamente difíceis de bloquear: Eles não podem ser evitadas pelo uso de configurações de privacidade do navegador da Web padrão ou o uso de ferramentas anti-rastreamento como AdBlock Plus.

Não acaba por ai, outras formas como o "Evercookies" (tradução livre, Cookies para sempre) utilizam-se de mecanismos ardilosos para serem instalados e são de difícil detecção e praticamente de impossível remoção tendo a mesma finalidade de extrair seus dados e redireciona-los para sites e empresas que irão compilar e revende-los.

Além de sites e redes sociais, até mesmo notebooks e smartphones através do indicador de bateria permite que alguém te espione pela internet, isto é feito pelo HTML5 que é uma linguagem de programação padronizada pela W3C uma organização de padronização da WWW (como se fosse a ABNT dos sites), que de acordo com o site inglês The Guardian[12] "permite que sites descubram a quantidade de bateria que resta no seu celular ou notebook com o objetivo de ajudar usuários a conservar bateria dos dispositivos, no entanto podem ser utilizado para rastrear os navegadores online, tudo isso sem a permissão do usuário."

Deste modo, como brevemente demonstrado e sem mais aprofundamentos na parte técnica concernente ao ramo da computação, observa-se que há inúmeras maneiras de adquirir informações utilizando dispositivos eletrônicos e técnicas informáticas que sequer dão ciência ao cidadão da exposição que tem que suportar, por exemplo, quando empresas de telefonia, tv a cabo e afins te ligam às 8:00 horas da manhã querendo vender um serviço, mas afinal, como sabem meu telefone? Dados como nome, CPF e endereço se nunca foram disponibilizados informações para aquela empresa?

Diante de tantas incertezas e da falta de legislação específica que iniba e aplique sanções aos que cometem lesões à direitos fundamentais e da personalidade se utilizando de meios tecnológicos, é que se faz necessário que o advento destas legislações abarque de forma pontual as possibilidades de infrações que são cometidas. No Brasil temos a Lei nº 12.965, de 23 de abril de 2014, popularmente conhecida como o Marco Civil da Internet, está longe de ser o ideal quando o assunto são crimes cometidos por meio tecnológico, mas é um ponto de partida a ser considerado para a confecção de leis próprias e rigorosas quanto aos crimes virtuais.

Enquanto isso, a sociedade tem que estar alerta e decidir até onde vale a pena abrir mão da privacidade para fazer parte da sociedade "big brother", pois mesmo que o indivíduo saiba que está sendo vigiado, de fato nunca poderá saber até onde esta vigilância o atinge, e portanto, onde aquele simples clique em "Like" ou aquele acesso ao site de receitas culinárias deixa de ser um momento de descontração para rotular com um código de barras aquele cidadão e transforma-lo em apenas mais um dado digital a ser vendido, exposto e desrespeitado.

4 CONCLUSÃO

Diante do exposto, é inequívoca a constatação que as análises feitas por Michel Foucault ao modelo Panóptico de Jeremy Bentham mesmo se tratando de mais de duas décadas passadas, bem como a visão futurística de George Orwell na obra "1984", enquadra-se perfeitamente nos dias contemporâneos, pode-se suspeitar que talvez até teriam uma "bola de cristal" para descrever de forma tão precisa os tempos vindouros.

O Panóptico que outrora era de concreto, hoje é de circuitos, chips, softwares e da mais vasta gama de dispositivos tecnológicos que vigia, coleta dados e expõe o cidadão constantemente. Tecnologia que ao chegar oferece mais "segurança", "comodidade" e "celeridade" no cotidiano das pessoas e também para seus lares. As câmeras de segurança, que nenhuma segurança traz, além de filmar o ocorrido, internet das coisas (Internet of Things), sua casa toda digital, acione pelo celular e deixe sua banheira enchendo enquanto sai do trabalho e chega em casa, que comodidade não?!

Assim como a moeda tem dois lados, tudo tem o lado bom e ruim, enquanto desfruta-se da sensação de segurança, comodidade e celeridade nada reclama-se da tecnologia, todavia, é para o lado ruim da "moeda" que o legislador e os cidadãos devem ficar atentos, pois os dispositivos tecnológicos sem nenhuma dúvida serão cada vez mais presente no dia a dia das pessoas, e legislações específicas devem ser elaboradas de forma a inibir que dispositivos eletrônicos não sejam meios e nem fins para cometimento de crimes.

[11] Tradução livre, informações extraídas do site: http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block
[12] Tradução livre, informações extraídas do site: http://www.theguardian.com/technology/2015/aug/03/privacy-smartphones-battery-life

Crimes através de dispositivos tecnológicos são cada dia mais frequentes, invasão a contas bancárias online, vigilância por drones, câmeras, *porn reveng*, *sexting* e inúmeros outros crimes que são cometidos por meios tecnológicos, mas que ao julgar os quem comete o ato ilicito, por não existir no ordenamento jurídico pátrio uma legislação própria, acabam estes, recebendo uma penalidade por analogia e que muitas vezes não atingem o caráter de disciplinar que a pena propõe.

O primeiro passo foi dado, através do Marco Civil da Internet (lei nº 12.965, de 23 de abril de 2014), mais este passo deve ser acelerado, pois sabe-se que a sociedade evolui em uma velocidade que o direito não consegue acompanhar, a tecnologia veio para acelerar ainda mais a evolução da sociedade e levá-la a outro patamar.

Assim sendo, resta aos nossos legisladores e aos operadores do direito que despertem para o assunto e comecem a trabalhar com afinco, como alguns já estão começando a fazer, através de projetos de lei como, o Projeto de Lei 5555/2013 (Maria da Penha Virtual) e também o Projeto de Lei 6630/2013 (*Porn Revenge*), entretanto, está longe de ser o aceitável visto a diversidade de ilicitudes que se pode cometer utilizando os meios e dispositivos tecnológicos em uma sociedade contemporânea cada vez mais líquida.

REFERÊNCIAS

ACAR, Gunes; EUBANK, Christian...[et al]. *The Web never forgets*: Persistent tracking mechanisms in the wild is the first large-scale study of three advanced web tracking mechanisms - canvas fingerprinting, evercookies and use of "cookie syncing" in conjunction with evercookies. Disponível em: https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html#. Acesso em 18 ago. 2015.

ANGWIN, Julia. *Meet the online tracking device that is virtually impossible to block*. Disponível em: http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block. Acesso em 15 de ago. 2015.

BAUMAN, Zygmunt. *Modernidade líquida*. Rio de Janeiro: Jorge Zahar, 2001.

BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Rio de Janeiro: Zahar, 2014.

BENTHAM, Jeremy; PERROT, Michelle...[et al]. *O panóptico*. 2. ed. Belo Horizonte: Autêntica Editora, 2008.

CONLEY, Chris. *The Social Network is Stalking You*. Disponível em: https://www.aclu.org/blog/speakeasy/social-network-stalking-you?redirect=blog/technology-and-liberty/social-network-stalking-you. Acesso em 15 ago. 2015.

HERN, Alex. *How your smartphone's battery life can be used to invade your privacy*. Disponível em: http://www.theguardian.com/technology/2015/aug/03/privacy-smartphones-battery-life. Acesso em 18 de ago. 2015.

MICHEL, Foucault. *Vigiar e punir*: nascimento da prisão. 20 ed. Petrópolis: Vozes, 1987.

ORWELL, George. *1984*. São Paulo: Companhia das Letras, 2009.

PORTAL BRASIL. Força Aérea esclarece normas para voos de drones no Brasil. Disponível em: http://www.brasil.gov.br/defesa-e-seguranca/2015/03/forca-aerea-esclarece-normas-para-voos-de-drones-no-brasil. Acesso em 18 de ago. 2015.