Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 02.02.2023
Aprovado em: 15.02.2023

INTELIGÊNCIA ARTIFICIAL E VIOLÊNCIA DOMÉSTICA: A GARANTIA À INTEGRIDADE FÍSICA POR MEIO DA RELATIVIZAÇÃO DA PRIVACIDADE.

ARTIFICIAL INTELLIGENCE AND DOMESTIC VIOLENCE: THE GUARANTEE OF PHYSICAL INTEGRITY THROUGH THE RELATIVIZATION OF PRIVACY.

Isabelle Brito Bezerra Mendes[*]

RESUMO

A presença massiva da tecnologia no cotidiano social tem alcançado níveis cada vez mais profundos da intimidade dos indivíduos, apontando para um evidente aumento na produção de dados pessoais e um constante monitoramento consentido. Assistentes virtuais e outros objetos inteligentes são capazes de captar mais informações sobre um indivíduo e suas preferências, ou sobre um ambiente do que uma testemunha ocular. Essa presença íntima da tecnologia seria uma alternativa viável no auxílio a vítimas de crimes domésticos e as informações obtidas relevantes na solução de casos. Seria, então, legalmente razoável e socialmente relevante a relativização da privacidade para a utilização de informações obtidas a partir de assistentes virtuais como prova válida em crimes domésticos? A resposta essa pergunta leva em consideração o conceito de privacidade, que por si só não é definitivo e a depender das alterações sociais e tecnológicas pode mudar; o fato de a presença de assistentes digitais nas casas das pessoas não representar por si só uma quebra de privacidade ou uma intrusão indevida; a necessidade do direito de proporcionar soluções pertinentes tanto em favor da preservação de direitos dos indivíduos, como eficazes no incentivo a inovação frente aos desdobramentos da inclusão tecnológica no cotidiano social, e a viabilidade da relativização da privacidade quando em conflitos com outros direitos (como a integridade física). Para que isso ocorra de forma organizada e prudente, o direito deve ter capacidade regulatória, não apenas tipificando crimes, como também abarcando as possibilidades advindas da tecnologia em relação a provas no processo penal.

Palavras-chave: Inteligência Artificial. Assistentes Virtuais. Crimes Domésticos. Prova Válida. Privacidade.

ABSTRACT

The massive presence of technology in everyday social life has reached increasingly deeper levels of individuals' intimacy, pointing to an evident increase in the production of personal data and constant consented monitoring. Virtual assistants and other smart objects are able to pick up more information about an individual and his or her preferences, or about an environment,

[*] Mestranda em Direito Constitucional pela Universidade Federal do Ceará (UFC). Especialista em Proteção de Dados pela Universidade de Fortaleza (UNIFOR). Coordenadora de Pesquisa do Grupo de Estudos em Tecnologia, Informação e Sociedade (GETIS). Pesquisadora do Núcleo de Pesquisa em Interpretação e Decisão Judicial (NUPID). Tax Consultant na Ernest Young. E-mail: isabellemendes06@gmail.com.

than an eyewitness. This intimate presence of technology would be a viable alternative in helping victims of domestic crimes and the relevant information obtained in solving cases. Would it then be legally reasonable and socially relevant to relativize privacy for the use of information obtained from virtual assistants as valid evidence in domestic crimes? The answer to this question takes into account the concept of privacy, which by itself is not definitive and may change depending on social and technological changes; the fact that the presence of digital assistants in people's homes does not itself represent a breach of privacy or an undue intrusion; the need for the right to provide relevant solutions both in favor of preserving the rights of individuals, as well as effective in encouraging innovation in the face of the unfolding of technological inclusion in social daily life, and the feasibility of relativizing privacy when in conflict with other rights (such as physical integrity). To this situation occur in an organized and prudent way, the law must have regulatory capacity, not only typifying crimes, but also embracing the possibilities arising from technology in relation to evidence in criminal proceedings.
Keywords: Artificial Intelligence. Virtual Assistants. Domestic Crimes. Digital Evidence. Privacy

INTRODUÇÃO

É inegável que o advento e desenvolvimento da tecnologia impactou, e assim continua, as diversas searas sociais, como a economia, com um melhor resultado dos estudos planejados, bem como a celeridade e aprimoramento dos processos que levam ao produto final; os transportes com o melhoramento da mobilidade das pessoas e encurtamento de distancias e, as comunicações com a possibilidade de rápida disseminação de informações e facilidade no contato entre os indivíduos. A maior parte dessas possibilidades apontadas há poucos anos estavam em fase primária ou eram apenas fruto de um imaginário ideal. Atualmente parece até impossível pensar a continuidade das atividades sociais sem elas.

O exposto, demonstra exatamente a posição intrínseca que a tecnologia tem ocupado no cotidiano das atividades humanas, e as alterações advindas dessa interação inevitavelmente pressionam o direito e o sistema jurídico por soluções e respostas que abarquem essas novidades e sejam adequadas a manutenção dos direitos e garantias fundamentais. Não há mais como retroceder do avanço tecnológico e por isso, não há como o direito continuar o mesmo. Não se fala apenas da necessidade de criação de leis específicas direcionando o uso da Internet, o tratamento de dados pessoais, ou mesmo o uso de Inteligência Artificial, mas principalmente a atualização dos textos infraconstitucionais já existentes.

Inevitavelmente, essa adequação jurídica a realidade social pode levar a um conflito de garantias fundamentais, o que é totalmente possível dentro da dinâmica jurídica, e, a depender do caso, um direito pode se sobrepor a outro. Esse, é exatamente o contexto do uso de informações coletadas por assistentes digitais como provas válidas em possíveis casos de violência doméstica, onde há uma sobreposição da integridade física frente a privacidade.

O presente trabalho, portanto, visa explicar a importância e entender a viabilidade dessa relativização da privacidade, vendo-a como uma possibilidade relevante no combate a um tipo penal pertinente em nossa sociedade, onde, muitas vezes, as vítimas ainda não têm o devido apoio ou, na maioria dos casos, são as únicas testemunhas da violência que sofreram. Além de ser um avanço para as discussões em torno das questões envolvendo Inteligência Artificial e sua efetiva normatização no Brasil. Portanto, busca-se responder a determinados questionamentos como: Como o desenvolvimento tecnológico impacta na compreensão do conceito de privacidade? De que maneira a relativização da privacidade pode contribuir no combate a crimes domésticos? A normativa brasileira atual possui disposições suficientes para abarcar essa realidade?

A justificativa para esse trabalho está exatamente no impacto da tecnologia no direito, que não pode ficar inerte aos avanços conquistados e pode aproveitar-se das possibilidades digitais surgidas a seu favor para a garantia de direitos dos indivíduos, principalmente no que se referem a crimes. Aqui há também que se mostrar que essa possibilidade não é de todo nova, levando em consideração as discussões ocorridas em alguns casos, como nos Estados Unidos que foram fundamentais para os debates iniciais das questões aqui tratadas.

Tem-se como objetivo geral verificar a viabilidade da utilização dos dados armazenados por assistentes virtuais como meios de prova válidos em crimes de violência doméstica, levando em consideração as questões sobre privacidade e preservação de direitos.

A metodologia utilizada no trabalho quanto a natureza se caracteriza como uma pesquisa bibliográfica, com a análise de livros, artigos, dissertações, e leis, com abordagem qualitativa buscando compreender o objeto em análise a partir da leitura de autores com domínio no assunto abordado, além da comparação com outros contextos. Trata-se de pesquisa

descritiva, por indicar conceitos, situações e os cenários aplicáveis ao objeto, e exploratória, por buscar maiores informações sobre o tema abordado.

Na primeira parte desse trabalho, há uma breve explicação sobre o desenvolvimento histórico-social do conceito de privacidade e como a tecnologia tem sido relevante nesse sentido. Em seguida há uma análise do desenvolvimento e crescimento do comércio de assistentes digitais, sua aproximação cada vez maior da intimidade humana, trazendo à tona a conivência humana dos usuários nesse sentido e como essa realidade tem gerado por si só uma contribuição na alteração da percepção dos limites de privacidade pelas pessoas. Por fim, levanta-se a discussão em torno da violência doméstica no contexto da sociedade atual e o impacto da privacidade em situações como essas, com a apresentação de casos ocorridos nos Estados Unidos e as discussões criadas a partir da solução das questões

Na segunda parte há uma breve análise do conceito de prova, até que se chegue a compreensão do que se trata a prova digital como se classificariam e como poderia ser aceita no processo penal brasileiro como válidas. Há em seguida a análise do projeto de lei brasileiro com diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo e sua viabilidade para a coleta de provas de assistentes digitais. Por fim, faz-se uma breve flexão sobre a responsabilidade jurídica, com alterações normativas, na condução do melhor direcionamento das ferramentas tecnológicas.

1 PRIVACIDADE E TECNOLOGIA

As discussões sobre privacidade não são recentes. Em 1890 o conceito de privacidade foi delineado por Samuel Warren e Louis Brandeis em um artigo intitulado *The Right to Privacy*, onde apontaram as alterações nos diversos segmentos da sociedade, bem como as inovações surgidas ao tempo, a exemplo da fotografia, como fatores de forte contribuição na violação da privacidade das pessoas. Tendo uma posição bem radical do que seria a privacidade indicando-a como “o direito de ser deixado só” (*the right to be alone*), um completo apoio ao individualismo e a pouca interação social (DONEDA, 2019, p.30).

Essa conceituação encaixou-se de forma oportuna para as “figuras públicas” do período, como Rainhas, príncipes e membros da alta sociedade, que por diversas vezes levavam

a julgamento seus casos visando impedir a exposição de suas vidas. (DONEDA, 2019, p.33). Por essa razão, o direito à privacidade nesse período parecia uma garantia apenas da elite e não das pessoas comuns.

Isso mudou após 1960, com o aumento do fluxo de informações resultado da massificação do uso de tecnologias e da facilitação de sua dispersão e de seu repasse, evidenciando assim a possibilidade da violação da privacidade de qualquer indivíduo. Nesse período, Alan Westin (1967, p.24-25) explicou que:

> Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outras pessoas. Vista em termos da relação do indivíduo com a participação social, a privacidade é a retirada voluntária e temporária de uma pessoa da sociedade em geral por meios físicos ou psicológicos, seja em estado de solidão ou intimidade de pequenos grupos ou, quando entre grupos maiores, em condição de anonimato ou reserva. O desejo de privacidade do indivíduo nunca é absoluto, pois a participação na sociedade é um desejo igualmente poderoso. (tradução nossa)

Tal colocação traz uma posição diferente da proposta por Warren e Brandeis, há aqui uma compreensão da vivência em sociedade dos indivíduos e que isso, por si só, impediria a total e completa proteção à privacidade. A partir daí, já se começa a observar a privacidade "na perspectiva do controle do indivíduo sobre o uso de suas informações pessoais por terceiros" (COSTA, 2019, p. 13). Os Estados começaram a perceber também que a posse de informações seria fundamental para o controle e domínio sobre as sociedades e melhor direcionamento das situações. Em seguida, os entes privados também começaram a utilizar informações pessoais para obtenção de vantagens em seus negócios e atividades, sendo agora uma ferramenta não só de controle social, mas principalmente de influência. (DONEDA, 2019, p.35-37)

Nos anos 70 a 90, acompanhando o acelerado desenvolvimento tecnológico e a rápida facilidade de coleta e disseminação de informações, as nações começaram a lançar legislações relativas à proteção de dados. Essa onda regulatória traz consigo o protagonismo do consentimento, cuja intenção é que o indivíduo seja capaz de escolher ou permitir a coleta, o uso e o compartilhamento de seus dados, tendo uma participação plena sobre o caminho que seus dados percorrem. (BIONI, 2019, p. 175). Portanto, seria a transferência de responsabilidade da proteção de dados do Estado para o próprio indivíduo, titular dos dados, direcionando-o para uma "autodeterminação informativa".

1.1 Impactos do desenvolvimento tecnológico na privacidade

O conceito de privacidade é influenciado pelo contexto social e pode mudar a depender das alterações sociais ocorridas e do desenvolvimento de novas tecnologias, conforme explica Daniel Solove (2008, p.4):

> Desde a antiguidade, as pessoas em quase todas as sociedades debatem questões de privacidade, desde fofocas até espionagem e vigilância. O desenvolvimento de novas tecnologias manteve a preocupação com a privacidade latente por séculos, mas a profunda proliferação de novas tecnologias da informação durante o século XX – especialmente a ascensão do computador – fez com que a privacidade se tornasse uma questão de primeira linha em todo o mundo. (tradução nossa)

E coaduna Danilo Doneda (2019, p.41):

> A privacidade nas últimas décadas reuniu uma série de interesses ao redor de si, o que modificou substancialmente o seu perfil. Assim, chegamos ao ponto de verificar, de acordo com a lição de Stefano Rodotà, que o direito à privacidade não mais se estrutura em torno do eixo "pessoa-informação-segredo", no paradigma da *zerorelationship*, mas sim no eixo "pessoa-informação-circulação-controle".

Com a presença inovação e da tecnologia no cotidiano humano, houve uma mudança de perspectiva. Inicialmente, havia uma corrida frenética pelo total isolamento de informações e preservação completa da vida privada. Agora, há entendimento de que a informação inevitavelmente irá circular e detalhes da vida irão ser expostos, mas que deve existir algum tipo de controle do percurso desse dado.

Essa alteração conceitual não passa despercebida, sendo palco frequente de discussões e debates de doutrinadores e estudiosos, como Robert Post (2000, p.1, tradução nossa), que explica: "A privacidade é um valor tão complexo, tão emaranhado em dimensões concorrentes e contraditórias, tão repleto de significados variados e distintos, que às vezes me desespero se ela pode ser abordada de maneira útil. " Apesar disso, Danilo Doneda (2019, p.101) explica que a indefinição do conteúdo referente ao direito à privacidade na verdade deve ser entendida como uma característica própria do que como um defeito por si só.

Portanto, isso prova que o estado de desenvolvimento da tecnologia influencia significativamente, trazendo possibilidades interessantes e melhorias relevantes ao contexto social que há anos atrás seriam inimagináveis ou até mesmo pensadas absurdas. Um exemplo é o uso do celular, com o qual é possível se mapear facilmente todo o dia de um indivíduo, por onde andou, o que comeu, com quem se encontrou etc. Todas as informações são produzidas

pelo próprio usuário livremente e de alguma forma o ajudaram a otimizar seu dia e suas experiências de vida. Há, portanto, espaço para que o dono de um telefone, que o comprou por livre e espontânea vontade, tenha expectativa de uma total privacidade? Uma completa segurança de que seus dados não serão espalhados ou compartilhados? A resposta a essa pergunta é "não".

Essa resposta vem, pois atualmente as pessoas tem revelado informações sobre si a terceiros frequentemente, seja para obter acesso a serviços, para entrar em eventos ou apenas para usufruir de produtos de última geração para sua comodidade (BUGEJA, JACOBSSON, DAVIDSSON, 2016, p.1). Cada vez mais essas informações têm se tornado mais íntimas, desde áudios completos de um ambiente até o padrão de fluxo menstrual de uma mulher. Isso significa necessariamente um rompimento de privacidade? Há alguns anos sim, de forma, talvez, até escandalosa. Hoje, já não se entende mais dessa forma. E, é exatamente nesse paradigma que se encontra a definição de privacidade.

Com essa reflexão não se quer dizer que não há limites para a guarda da privacidade, ou muito menos que ela está em total segundo plano nos últimos tempos com a realidade tecnológica vivida. Do contrário, se quer apenas explicar que a privacidade não é um conceito totalmente fechado e que muitas vezes sua definição e compreensão dependerá do contexto analisado e da sua comparação e confronto com outros direitos fundamentais.

1.2 Inteligência Artificial e vida privada

Segundo análises recentes há previsão de que mercado latino americano de soluções de Internet das Coisas (IoT) deverá movimentar mais de US$ 30 bilhões até 2023[1], além de que no Brasil é previsto que volume de dispositivos móveis ligados a IoT alcance a marca de 100 milhões[2], isso deve gerar um impacto anual US$ 50 bilhões e US$ 200 bilhões em 2025[3]. Tais

[1] Disponível em: https://tiinside.com.br/09/02/2022/internet-das-coisas-abinc-elenca-as-principais-tendencias-da-tecnologia-para-os-proximos-anos/#:~:text=Em%20conformidade%20com%20um%20relat%C3%B3rio,a%20marca%20de%20100%20milh%C3%B5es. Acesso em 20 de junho de 2022.

[2] Disponível em: https://tiinside.com.br/09/02/2022/internet-das-coisas-abinc-elenca-as-principais-tendencias-da-tecnologia-para-os-proximos-anos/#:~:text=Em%20conformidade%20com%20um%20relat%C3%B3rio,a%20marca%20de%20100%20milh%C3%B5es. Acesso em 20 de junho de 2022.

[3] Disponível em: https://tiinside.com.br/09/02/2022/internet-das-coisas-abinc-elenca-as-principais-tendencias-da-tecnologia-para-os-proximos-

dados, comprovam o alto interesse das pessoas, principalmente a população brasileira, em soluções tecnológicas para o seu dia a dia e dispostos a obtê-los, mesmo sabendo que irão adentrar um nível a mais em sua intimidade.

Vale explicar que IoT é o termo genérico e mais utilizado para indicar objetos em casas, ambientes profissionais, empresas, e cidades que "vêm sendo conectados à Internet e adquirindo diversos níveis de inteligência e capacidade de processamento" (COSTA, 2019, p. 6). Ou seja, não são apenas produtos capazes e coletar dados em rede, mas de realizar todo um processamento inteligente dessas informações, de forma a aprimorar seu desempenho mediante as experiências obtidas. Vale ressaltar que normalmente o processamento de comandos ocorre em grande parte no "*back-end*" baseado em nuvem do fabricante do dispositivo (LAU, ZIMMERMAN, SCHAUB, 2018, p.103).

Há, portanto, na realização desses serviços, constante mapeamento de atividades e monitoramento de comportamentos, perfilização (*Profiling*) de usuários e até o frequente uso de decisões automatizadas. Como exemplo desses produtos e serviços citamos, carros autônomos, sensores industriais, cidades inteligentes e assistentes digitais.

O interesse desse trabalho repousa especificamente nas assistentes digitais, das quais são exemplos comuns a *Alexa* da Amazon, a *Google Assistant* da *Google*, a Siri da *Apple* e a Cortana da Microsoft, as quais são frequentemente utilizadas no melhoramento do desempenho de atividades ou somente na automação de tarefas simples para comodidade do usuário. Sendo que para isso, uma quantidade significativa de dados é necessária, então, de forma consentida, o usuário permite a presença de um serviço prestado por terceiro capaz de coletar e armazenar todas as consultas do usuário, bem como quaisquer comentários inadvertidamente feitos (ALLEN, 2018, p.163).

Esse armazenamento é, inclusive comprovado pela Amazon, nos termos de uso da Alexa, quando diz:

> A *Alexa* é um serviço continuamente aprimorado que você controla com a sua voz. Quando você interage com a *Alexa*, ela grava e envia áudio para a nuvem. A *Alexa* está constantemente aprendendo e tornando-se mais inteligente. Ela se atualiza automaticamente por meio da nuvem para adicionar novos recursos e funcionalidades.

anos/#:~:text=Em%20conformidade%20com%20um%20relat%C3%B3rio,a%20marca%20de%20100%20milh%C3%B5es. Acesso em 20 de junho de 2022.

> Para fornecer o serviço *Alexa*, personalizá-lo e melhorar nossos serviços, a *Amazon* processa e armazena na nuvem suas Interações com a *Alexa*, tais como suas entradas de voz, suas listas de reprodução de músicas e suas listas de tarefas e de compras da *Alexa*. Saiba mais sobre a *Alexa*, inclusive sobre como excluir gravações de voz associadas à sua conta e gerir o nosso use de tais gravações de voz. (Grifos nossos)

Ou seja, o usufruto do produto e serviço está ligado a uma abertura na privacidade do usuário, que muitas vezes aceita sem nem mesmo ter total compreensão do que isso poderia significar. Sobre isso, Camelia Daciana Stoian, traz a seguinte explicação e uma reflexão relevante:

> As assistentes virtuais são bens móveis percebidos como uma compra útil e de saída sob a condição de que se tornem, pelo menos à primeira vista, uma propriedade exclusiva. Um relógio de pulso que indica o número de passos realizados diariamente, que mede nossa pressão arterial, nível de açúcar no sangue, pulso ou indica a rota, que nos avisa se estamos parados por um longo período de tempo ou um *gadget* que pode responder às nossas curiosidades diárias ou nos relaxa tocando nossa música favorita, nos dá o direito de sermos os orgulhosos donos do direito de possuir, usar e dispor dela de forma compreensível como exclusiva e absoluta. Mas, conhecemos os limites deste exercício de tal direito de propriedade, ou fomos devidamente informados previamente deste facto particular antes de pagarmos o preço? Estamos realmente cientes da forma como a resposta imediata à nossa pergunta é formada, as categorias de informações fornecidas sobre nós através das quais a experiência e as funções do dispositivo são aprimoradas em nosso interesse ou quem está coletando e processando esses dados que avaliam determinados aspectos pessoais? De que forma e em que medida o dispositivo reconhece o que queremos e nos dá a resposta desejada? Todas essas questões devem ser incluídas em algumas informações preliminares e, em nenhuma circunstância, devem fazer parte de uma decisão de processamento automático, incluindo também a criação de novos perfis que possam nos afetar e sobre os quais não temos nenhum direito de controle. (STOIAN, 2019, p. 135-136, grifo e tradução nossa)

Com o advento do capitalismo e a forte impulsão ao modelo de consumo constante, os consumidores normalmente não refletem a fundo sobre os desdobramentos do uso de determinados serviços e produtos. Muitas vezes, movidos pela necessidade de se ter o item da moda, e ter a experiência que se propõe a entregar, apenas se faz a compra e leva-se o objeto para o cotidiano. Ao pensar sobre isso, talvez algumas pessoas possam começar a repensar o uso de seus dispositivos tecnológicos, desenvolver uma série de questionamentos que envolve a proteção de seus dados ou até mesmo alimentar medos e teorias conspirativas radicais. E essa não é a intenção aqui, mas há que se colocar no debate que a adesão das pessoas a tecnologia muitas vezes se dá pela emoção que a posse do produto proporciona e não certamente de uma análise racional da necessidade do produto.

Os consumidores, portanto, oscilam entre a ideia de aceitar a vigilância e possíveis quebras de privacidade, mas não fazem nada nesse sentido e acabam colocando em primeiro

plano a utilidade de um *smart speaker*, e a ideia de se opor ao monitoramento sem sequer ter um procedimento em mãos a esse respeito (STOIAN, 2019, p. 137). Entretanto, há que se esclarecer que é uma realidade e não há mais como voltar, de modo que assistentes virtuais e celulares se tornem-se inutilizáveis. Em verdade, o que deve ocorrer, é o entendimento dos desdobramentos dessa realidade e como ela deve ser enfrentada de forma que, apesar das mudanças comportamentais e da presença desses dispositivos no cotidiano das pessoas, os seus direitos e garantias fundamentais sejam mantidos.

A Constituição Brasileira, em seu artigo 5°, XI, explica que "casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador", a intenção do constituinte foi evitar intrusões indevidas no lar, já que deveria ser o local de maior vulnerabilidade de um indivíduo. Mas, frente a realidade de uma *Smart Home*, onde os dados produzidos serão necessariamente espalhados por diversas bases de dados, devido à presença consentida de um serviço, a interpretação permanecerá a mesma frente a essa realidade? Haverá outros mecanismos para regular essa presença? A existência dessa atividade inovadora deve gerar por si só uma corrida desenfreada pela segurança completa das informações ou da margem para usos inovadores em questões sociais, econômicas, jurídicas e políticas? É o que se pretende analisar mais à frente.

1.3 Desenvolvimento digital, privacidade e crimes

Seria imprudente não mencionar que o desenvolvimento da tecnologia também abre portas para ações criminosas mais elaboradas, pode possibilitar variações de violações já mapeadas e, é um canal para criação de novos tipos penais.

Desde o advento da internet, por exemplo, e principalmente depois da acessibilidade de posse de um celular e consequentemente de redes sociais, notícias de *Cyberbulling*, *Fake News*, *Deep Fake*, *Phishing*, *Ransomware*, *Malware*, Pornografia, Violência de gênero e psicológica, Estelionatos, entre outros tem sido recorrente. Entretanto, apesar do surgimento de crimes no contexto da rede e da conectividade, há outros tipos penais, existentes desde os primórdios, que até pouco tempo ainda permaneciam intocados pela tecnologia, e estavam seguros velados no silêncio e na privacidade que as "quatro paredes" proporcionam, até que a

inovação nos levou a ter em nossos celulares, e agora em nossas casas, assistentes digitais. E essa é uma outra perspectiva no que diz respeito à presença de dispositivos eletrônicos na intimidade de indivíduos.

Quando se olha sob essas lentes no contexto da violência doméstica, talvez seja possível entender um pouco da relevância dessa entrada da tecnologia no âmbito privado, já que normalmente a vítima seja a única fonte de provas, ou testemunha, do abuso sofrido (SOBERDASH, 2020, p.4), além de não terem o acolhimento devido quando buscam ajuda. A 3ª edição do relatório "Visível e Invisível: A vitimização das mulheres no Brasil"[4], elaborado pelo Fórum de Segurança Pública em parceria com o Datafolha e patrocínio da Uber, traz um pouco dessa realidade ao expor que:

> Ao longo dos meses de abril, maio e junho de 2020, em uma parceria com o Banco Mundial, o FBSP lançou três notas técnicas, que buscaram compilar estatísticas oficiais das Unidades da Federação sobre o assunto. Essas notas identificaram, resumidamente, que durante o período monitorado houve queda nos registros policiais de lesão corporal dolosa, ameaça, estupro e estupro de vulnerável contra mulheres. Em sentido contrário, a violência letal – feminicídio e homicídio de mulheres - apresentou crescimento no período, em um sinal de agravamento dos conflitos. (BRASIL, 2020, p. 7-8)

Um dado a ser considerado e que reforça o entendimento de que a privacidade e a impenetrabilidade da casa, durante a Pandemia de Covid 2019 principalmente, foi ou é um fator favorável aos agentes em crimes domésticos e totalmente devastador para a vítima. Portanto, informações de um dispositivo virtual podem ser relevantes na solução de casos, com provas insuficientes, bem como podem ser determinantes para auxiliar na melhoria de nossa realidade social.

Sobre isso, Tabetha Soberdash (2020, p.3) traz um interessante questionamento: "E se a tecnologia de casas inteligentes também pudesse ser usada para ajudar sobreviventes de violência doméstica? " Vale ressaltar que nas informações obtidas nesses dispositivos há um grande diferencial, já que os fatos foram fidedignamente gravados e os dados foram produzidos pelo próprio responsável pelo crime. Lindsey Freeman (2017, p.283) esclarece que os dispositivos digitais são capazes de capturar muito mais informações sobre uma situação do que um humano seria capaz. Ou seja, dados esclarecedores e suficientes para solucionar uma

[4] Disponível em https://forumseguranca.org.br/publicacoes_posts/violencia-domestica-durante-pandemia-de-covid-19-edicao-03/. Acesso em 26 de junho de 2022.

questão.

1.3.1 Cases

É certo que não se pode trazer toda a perspectiva anteriormente apresentada apenas no plano teórico, já que a prática é fundamental para se entender a real viabilidade do que se fala. Frente a isso vale trazer alguns casos interessantes onde dispositivos eletrônicos e assistentes digitais foram fundamentais na elucidação de crimes.

O primeiro trata-se do caso James Bates vs Victor Collins[5], em 2015. Na ocasião, Bates foi acusado de assassinato pela morte de Collins, em um evento ocorrido em sua casa. O caso foi arquivado em 2017, após a obtenção das informações da *Alexa* de Bates, da noite do crime, que trazem evidencias suficientes para pôr em dúvida a autoria do crime por Bates. Vale ressaltar que nesse caso, inicialmente a *Amazon* se recusou a fornecer as informações, mas como o dono do dispositivo informou que iria autorizar a entrega voluntária das gravações, a empresa disponibilizou o conteúdo armazenado.

Outro caso intrigante envolve o uso de um Fitbit. A vítima era Nicole VanderHeyden[6], que foi assassinada, tendo como principal suspeito seu namorado, que foi salvo devido as informações contidas em seu "smart watch", que afastaram as suspeitas sobre ele. Entretanto, o novo suspeito, George Buch, foi descoberto devido aos dados coletados de seu celular, onde seu *Google Dashboard* indicou que teria estado exatamente no mesmo local do crime de Nicole. Além de que o histórico de navegação mostrava que tinha lido muitas vezes notícias sobre o crime envolvendo Nicole.

O último caso e talvez um dos mais relevantes aqui é exatamente o Microsoft Corp. v. United States[7] onde em 2013 o magistrado emitiu um mandado sob o *Stored Communications Act* (SCA) para obtenção de um conteúdo associado a um endereço de e-mail Microsoft Network (MSN). Entretanto, a Microsoft entregou apenas os dados armazenados nos Estados Unidos e, na realidade muitas das informações solicitadas estavam armazenadas em um

[5] Disponível em https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html. Acesso em 26 de junho de 2022.
[6] Disponível em: https://www.greenbaypressgazette.com/story/news/crime/2021/06/29/state-supreme-court-upholds-george-burch-murder-nicole-vanderheyden/7796513002/. Acesso em 26 de junho de 2022.
[7] Disponível em: https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/. Acesso em 26 de junho de 2022.

servidor da Microsoft na Irlanda. A Microsoft decidiu anular o mandato argumentando que os dados da Irlanda estavam além da jurisdição da ordem emitida.

Nesse caso foram levantadas discussões envolvendo apenas a questão da extraterritorialidade, que perdurou até o fim do processo, inclusive levando a não obtenção dos dados. Mas o fato é que nesse caso travou-se uma discussão tão longa sobre territorialidade e na verdade foi deixado de lado as análises sobre os atributos dos dados, que são fluidos e que por sua natureza não pertencem mesmo a apenas um território. Sobre isso a Harvard Law (2016) traz um posicionamento elucidativo:

> Quando os tribunais precisam aplicar leis antigas à tecnologia moderna, eles enfrentam uma escolha: podem tratar a tecnologia como fariam com qualquer outra coisa, ou podem reconhecer suas qualidades únicas e considerar adaptar sua aplicação das leis existentes de acordo.

Que inclusive coaduna com o posicionamento de Orin S. Kerr (2013, p.403) de que:

> Mudanças Tecnológicas reapresentam um problema recorrente para os legisladores. As leis são promulgadas com uma compreensão fundamental dos fatos. Quando esses fatos mudam, o efeito das antigas regras legais pode mudar junto com elas. Uma lei criada para um mundo pode ter um impacto muito diferente quando aplicada aos fatos de uma época diferente. Como resultado, mudanças tecnológicas e de práticas sociais pode desencadear uma necessidade de adaptação legal. Manter a função de regras antigas pode exigir alterar regras para adaptar ao novo ambiente. (tradução nossa)

Ou seja, muitas vezes a solução de casos e situações dessa geração não poderão ser resolvidos pela mera aplicação de leis criadas em um contexto totalmente oposto, pois não serão suficientes para abarcar o cerne do problema e apenas trarão à tona discussões que em nada serão proveitosas. Por isso, o direito precisa acompanhar as mudanças ocorridas e desenvolver mecanismos que não apenas previnam situações ilegais dentro do contexto digital, mas que também auxiliem o meio jurídico na promoção e proteção coerente de garantias e direitos fundamentais.

2 RELATIVIZAÇÃO DA PRIVACIDADE NO CONTEXTO NORMATIVO BRASILEIRO

A economia capitalista trouxe as sociedades muitas vantagens e melhorias para o cotidiano social, mas ao mesmo tempo trouxe desafios e alterações relevantes as quais o direito precisa acompanhar. Sobre essa questão, Jeffrey Sachs (1998, p.2) traz uma análise interessante:

> A confluência da globalização e a disseminação do capitalismo está produzindo uma sociedade de mercado global de caráter único, ainda vagamente percebida, e com instabilidades e desafios próprios de nossa época. [...] É na esfera jurídica que encontramos muitas das mais profundas fraquezas e maiores esperanças para nossa época. É nos processos do direito, talvez mais do que nas instituições econômicas, que residem os maiores enigmas do enfrentamento de nossas sociedades.

Apesar da compreensão fundamental da necessidade que o meio jurídico tem de se adaptar à realidade tecnológica vivida, trazer o uso da prova digital para o processo não é um trabalho tão simples. Isso em razão da lacunosidade de leis que versem sobre a admissibilidade de evidências digitais obtidas de assistentes digitais, como também das objeções a esse tipo de prova, onde se argumenta o possível abalo a expectativa de privacidade de uma pessoa e seus direitos constitucionais (SOBERDASH, 2020, p.5)

No que se refere especificamente a privacidade, há um claro conflito de direitos, no caso à vida privada versus à integridade física de uma vítima. Nesses casos, é sabido que não existem direitos absolutos, conforme foi reconhecido pelo STF[8], e as informações sobre o caso concreto são determinantes para definir a preponderância de um direito sobre outro[9]. Entretanto, no que se referente a inserção da prova digital ao processo há uma série de fatores a serem levados em consideração que deixam a discussão mais longa.

2.1 A prova digital e sua admissibilidade ao processo

O processo penal brasileiro, em seu modelo acusatório, prima pela busca da verdade formal, tendo como base a estrita legalidade, bem como a relevância da produção probatória para a condução de um processo devido, garantindo-se o contraditório e a ampla defesa de suas partes. Ademais, o Código de Processo Penal em seu Artigo 155[10] explica que o juiz deverá

[8] STF, MS 23.452-RJ, rel. Min. Celso de Mello. "mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição".

[9] "As normas constitucionais são potencialmente contraditórias, já que refletem uma diversidade ideológica típica de qualquer Estado Democrático de Direito. Não é de se estranhar, dessa forma, que elas frequentemente, no momento aplicativo, entrem em "rota de colisão". [...] Qualquer solução a ser adotada em um conflito assim resultará na restrição (às vezes, total) de um dos dois valores. [...] Todas as situações envolvendo o fenômeno da colisão de direitos fundamentais são de complexa solução. Tudo vai depender das informações fornecidas pelo caso concreto e das argumentações apresentadas pelas partes do processo judicial. Daí por que é preciso partir para a ponderação para solucionar esse conflito." (MARMELSTEIN, 2019, p. 373)

[10] BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 de junho de 2022.

formar sua convicção pela livre apreciação da prova devidamente produzida em contraditório judicial. Portanto, prova é o meio pelo qual é formada a convicção do juiz em relação a um fato específico (THAMAY; TAMER, 2022, p.28) e, não é toda prova que pode ser levada em consideração, mas tão somente aquelas que estiverem de acordo com a formalização adotada pela lei, e para isso são levadas em consideração a prova em si e sua relevância para o caso, seu meio de obtenção e sua produção.

A prova, portanto, deve ter estrita ligação com o fato, deve ser obtida dentro dos padrões legais, bem como deve ser advinda de uma fonte válida. Fora disso, segundo o Artigo 157 do Código Penal[11], as provas são passíveis de inadmissibilidade no contexto processual. Aury Lopes Junior (2011) explica que, pode-se aceitar excepcionalmente provas atípicas, desde que dentro dos limites constitucionais e processuais. Dessa forma, essas provas não podem extrapolar os direitos e garantias fundamentais das partes e devem ser proporcionais ao contexto.

No que se refere especificamente aos limites constitucionais, é importante lembrar que a viabilidade probatória, por si só, é um direito garantido constitucionalmente[12] como meios e recursos inerentes a garantia do contraditório e da ampla defesa, e como salientam Rennan Thamay e Maricio Tamer (2022, p. 18):

> A prova deve ser viabilizada de acordo com as configurações com o que o fato a ser provado se apresenta. Enquanto direito constitucional fundamental, tal premissa não pode ser desconsiderada às partes, sobretudo sob, por vezes, o argumento utilizado – e frágil, a nosso ver – da ausência de um meio típico de prova.

Com isso, a prova não pode ser desconsiderada apenas em razão de sua atipicidade, em se tratando de um direito constitucional e se lícita para provar os fatos do caso, o direito deve dar suporte à recepção da prova.

No que se referem especificamente as provas digitais, não há na lei menção direta a elas, por essa razão possivelmente deverão ser aceitas como provas atípicas, devendo passar pela aferição acima mencionada (VAZ, 2012, p. 60). O conceito de prova digital não é simples, mas duas acepções são possíveis segundo Thamay e Maricio Tamer (2022, p. 32):

[11] BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 de junho de 2022.
[12] Art. 5°, LV, CF/1988

> Uma primeira, segundo a qual a prova digital pode ser entendida como a demonstração de um fato ocorrido nos meios digitais, isto é um fato que tenha como suporte a utilização de um meio digital. E, uma segunda, em que, embora o fato em si não tenha ocorrido em meio digital, a demonstração de sua ocorrência pode se dar por meios digitais.

São, portanto, meio de demonstração de uma situação ocorrida dentro de um meio digital, ou que a partir do digital como instrumento podem ser relevantes para explicar um fato. Vale salientar que não se deve confundir com a prestação de informações feita por meio eletrônico. Vale ressaltar, que a prova digital tem características próprias que devem ser levadas em consideração, principalmente no que diz respeito ao seu registro, extração, conservação e apresentação em juízo, pois são elas que individualizam como categoria específica de fonte de prova (VAZ, 2012, p. 63).

Levando-se em consideração o exposto é necessário que a prova digital seja analisada com cautela e que possua regras direcionadas para que sejam aproveitadas da melhor forma possível.

2.1.1 Lei de Interceptação Telefônica

Apesar do exposto, inicialmente pode se pensar que a Lei n° 9.296 (Lei de Interceptação Telefônica) seria apropriada nessa situação, já que trata especificamente de interceptação do fluxo de comunicações em sistemas de informática, e como as assistentes virtuais fazem gravação dos sons do ambiente, intuitivamente pode-se crer que seria um ato abarcado por essa lei. Especialmente em seus Artigos 10 e 10-A:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei [...] Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei.
> Art. 10-A. Realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial, quando esta for exigida [...]

Ocorre que, esses dispositivos não englobam especificamente as gravações feitas por assistentes digitais, as quais seriam consideradas ilegais se aplicada a literalidade dessa lei, já que é uma escuta ambiental, feita sem autorização judicial, e sem objetivos claramente legais.

No caso das assistentes digitais, dois tipos de informações podem ser captadas, a primeira seria a ação criminosa por si só, o fato ilícito, e a segunda confissões de alguém sobre

o cometimento de um fato ilícito ou até mesmo padrões e históricos armazenados que podem ser cruciais.

Na obtenção do primeiro tipo de informação, não há expectativa de proteção de intimidade e privacidade, já que o Artigo 5°, XI da Constituição autoriza a entrada no domicílio alheio em caso de flagrante delito. Aqui, seriam necessários mecanismos normativos que apenas possibilitassem a solicitação as empresas o acesso a seus dados armazenados.

Na obtenção do segundo tipo de informação há uma complexidade maior. Pode se questionar inicialmente se o consentimento dado pelo titular dos dados nesse caso, baseado no que prevê a Lei Geral de Proteção de Dados, não seria suficiente para que se configurasse a licitude da prova para que seja utilizada. A resposta depende.

Em caso de informações de terceiros, por exemplo, é importante considerar que não se pode dar consentimento além do que a sua própria titularidade permite, ou seja os dados pessoais de outros, que estavam no ambiente, e foram captados não são abarcados pelo consentimento do titular, portanto teriam sido coletados indevidamente. Entretanto, no caso de informações do próprio titular, o consentimento poderia ser suficiente para configurar uma coleta lícita e passível de ser utilizada como prova. Mas, conforme explicamos anteriormente, não existem ainda mecanismos que reconheçam esse tipo de prova como válidos, bem como não há disposições normativas que direcionem a coleta dessas provas.

2.2 Projeto de Lei 4.939/2020

Frente ao exposto anteriormente, o Brasil tem buscado uma solução, está ainda em tramitação um projeto de lei[13] que visa dispor as normas de obtenção e admissibilidade de provas digitais na investigação e no processo.

Em seu artigo 4° já traz a definição de prova digital como “toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório. ” Na qual, as provas advindas de uma assistente digital poderiam se encaixar sem mais problemas.

[13] Projeto de Lei n° 4939/2020

No artigo 5° traz explicações sobre a admissibilidade da prova digital, onde se exigirá "a disponibilidade dos metadados e a descrição dos procedimentos de custódia e tratamento suficientes para a verificação da sua autenticidade e integridade. " Aqui será necessário que a prova seja passível de obtenção e que seja viável a verificação de sua autenticidade.

No que se refere a possibilidade de acesso aos dados de uma assistente virtual os Artigos 9° e 12° trazem a seguinte previsão:

> Art. 9º Constituem meios de obtenção da prova digital, na forma da Lei:
> I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo.
> II – a coleta remota, oculta ou não, de dados em repouso acessados à distância.
> III – a interceptação telemática de dados em transmissão.
> IV – a coleta por acesso forçado de sistema informático ou de redes de dados.
> V – o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.
>
> Art. 12 A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle.

Ou seja, num caso de necessidade de acesso as gravações da uma Alexa, por exemplo, o juiz deverá solicitar que a Amazon entregue as informações, entretendo, havendo negativa do pedido, poderia direcionar o acesso forçado as informações para que seja obtida prova. Tal situação por si só já demonstraria um resultado bem diferente do que foi exposto no caso da *Microsoft Corp. v. United States*.

Apesar de demonstrar perspectivas promissoras, o Projeto ainda não foi aprovado e não previsão para que isso ocorra. O que demonstra que apesar das boas intenções em atender uma necessidade real, não há o devido impulso para que ocorra com mais celeridade.

CONCLUSÃO

Diante do exposto, é possível entender que o conceito de privacidade por si só é mutante e altera-se de acordo com a realidade social vivida, sendo diretamente influenciado

pelo desenvolvimento tecnológico. Por essa razão, nos últimos anos tem ocorrido aumento da produção de dados, bem como um maior compartilhamento de informações a terceiros em troca de serviços e produtos que visam o bem-estar e a facilitação da vida cotidiana. Tudo isso, devido principalmente a necessidade capitalista de acompanhar e aderir a inovação.

Por um lado, toda essa situação gera um despertamento para a possível vulnerabilidade que as pessoas estão se colocando e então questionamento em relação a privacidade e sua proteção. Por outro lado, apesar da importância da garantia do direito à privacidade, não há que se criar uma expectativa de que se retornará a protege-la de forma total e completa, afinal a vida em sociedade por si só já impede isso. Ademais, não há como refrear o uso de celulares, assistentes digitais, relógios inteligentes, ou carros inteligentes para retornar a um completo anonimato em relação a produção e veiculação de dados.

Nesse contexto, há então que se perceber as possibilidades advindas dessa presença tão íntima da tecnologia na vida dos indivíduos e como podem ser úteis ao direito. Assim, uma assistente virtual poderia mudar a vida de uma vítima de violência doméstica, que normalmente não consegue e desvencilhar da situação por falta de provas suficientes para incriminar seu agressor, ou mesmo o apoio devido nesse sentido. A violência doméstica ainda é uma realidade em nossa sociedade e que é favorecida com o aumento dos muros da privacidade, relativizar um pouco esse direito seria uma alternativa importante no auxílio aos violentados, como se pode ver nos casos ocorridos nos Estados Unidos.

Das análises feitas ao longo do texto, é possível compreender também que há viabilidade do reconhecimento da prova digital como válida em um processo e assim, uma relativização da privacidade dos indivíduos envolvidos em prol da vítima e sua integridade física. Entretanto, essa realidade não está totalmente consolidada, apesar de ser possível, principalmente em caso de flagrante delito, não há mecanismos normativos suficientes que direcionem melhor o acesso as informações e aos dados coletados. É preciso que as discussões nesse sentido sejam melhor impulsionadas e que o direito coloque em pauta de forma mais frequente a realidade que a tecnologia traz.

A possibilidade de relativização da privacidade nesses casos não virá se essa questão não for levantada ou estiver pelo menos em pauta nos debates sociais. E aqui traz-se um posicionamento mais cético no que se refere aos reflexos do direito na impulsão do

desenvolvimento.[14] Visto que o Brasil, apesar de ser signatário da Convenção de Budapest, ter promulgado o Marco Civil, a Lei Geral de Proteção de Dados e algumas outras leis que versam sobre o cenário digital, ainda se encontra atrasado nesse sentido. Há muitas lacunas a serem preenchidas.

Para isso é necessário que as pessoas estejam minimamente cientes da realidade de seus dados frente a tecnologia, que tenham mais informações e sejam melhor educadas nesse contexto. A mudança tecnológica por si só pode gerar a necessidade de um melhoramento e de uma revisão normativa, mas se essas alterações não forem do interesse social, ou se os indivíduos não forem conscientes de como irá beneficia-los, a lei não fará o efeito desejado.

Portanto, o uso de informações advindas de assistentes digitais no contexto de violência doméstica apresenta-se como uma alternativa razoável e viável. Entretanto, só será possível mediante um efetivo acompanhamento normativo que abarque essa realidade, sem causar lacunas, além do apoio social para que o Estado efetivamente tome providências.

[14] Levando em consideração a análise feita por Kevin Davis e Michael Trebilcok em A Relação entre direito e desenvolvimento: Otimistas versus Céticos.

REFERÊNCIAS

ALLEN, Susan. Privacy in the Twenty-First Century Smart Home. **J. High Tech. L.**, v. 19, p. 162, 2018.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. [*S. l.*]: Editora Forense, 2019. 326 p. ISBN 8530981685.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1998**. BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, DF: Presidência da República, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 de junho de 2022.

BRASIL. Forum Brasileiro de Segurança Pública. **Visível e Invisível:** A Vitimização das Mulheres no Brasil. 3. ed. São Paulo, 2020. Disponível em: https://forumseguranca.org.br/publicacoes_posts/violencia-domestica-durante-pandemia-de-covid-19-edicao-03/. Acesso em: 26 jun. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais, de 14 de agosto de 2018. Brasília, DF: Presidência da República, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 abril 2022.

BUGEJA, Joseph; JACOBSSON, Andreas; DAVIDSSON, Paul. On privacy and security challenges in smart connected homes. **In: 2016 European Intelligence and Security Informatics Conference (EISIC)**. IEEE, 2016. p. 172-175.

COSTA, Manuella de Farias Nardelli. Internet das coisas: a proteção da privacidade em um mundo conectado. 2019.

DAVIS, Kevin E.; TREBILCOCK, Michael J. A relação entre direito e desenvolvimento: otimistas versus céticos. **Revista Direito GV**, v. 5, p. 217-268, 2009.

DONEDA, Danilo. **Da Privacidade À Proteção De Dados Pessoais**: Fundamentos da Lei Geral de Proteção de Dados. 2. ed. Revista dos Tribunais. São Paulo, 2019.

KERR, Orin S. Accounting for technological change. **Harv. JL & Pub. Pol'y**, v. 36, p. 403, 2013.

LAU, Josephine; ZIMMERMAN, Benjamin; SCHAUB, Florian. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. **Proceedings of the ACM on Human-Computer Interaction**, v. 2, n. CSCW, p. 1-31, 2018.

LOPES JR, Aury. Direito Processual Penal e Sua Conformidade Constitucional. Rio de Janeiro, Lumen Juris, 2011.

POST, Robert C. Three concepts of privacy. **Geo. LJ**, v. 89, p. 2087, 2000.

SACHS, Jeffrey. Globalization and the Rule of Law. 1998.

SOLOVE, Daniel J. Understanding privacy. 2008.

STOIAN, Camelia Daciana et al. Affecting the Right of a Private Life Through the Use of the Virtual Assistance. **Journal of Humanistic and Social Studies**, v. 10, n. 2, p. 135-142, 2019.

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. Tese de Doutorado. Universidade de São Paulo.

WESTIN, Alan. Privacy and Freedom. Nova Iorque, 1967.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy.** Columbia University Press, 1989.

THAMAY, Rennan; TAMER, Mauricio. Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie. 2ª Edição. **São Paulo: Thomson Reuters Brasil**, 2022.