INVASÃO DE DADOS POR DISPOSITIVOS ONLINE E ASSISTENTES VIRTUAIS E SUA VALIDADE COMO MEIO DE PROVA NO PROCESSO PENAL BRASILEIRO

Ana Claudia Bosrsato Orsi[1]
Alessandro Dorigon[2]

ORSI, A. C. B.; DORIGON, A. Invasão de dados por dispositivos online e assistentes virtuais e sua validade como meio de prova no Processo Penal Brasileiro. **Revista de Ciências Jurídicas e Sociais da UNIPAR**. Umuarama. v. 24, n. 1, p. 97-116, jan./jun. 2021.

RESUMO: Objetivou-se com o presente trabalho analisar se os dados obtidos por dispositivos *on-line* e assistentes virtuais, esses dotados da inteligência artificial, seriam válidos no âmbito processual penal brasileiro como meio de prova em um processo crime. Embora a virtualidade possa ser enquadrada aos demais ramos do direito, interessou-se desenvolvê-la no processo penal, pois, ao considerar que para seu pleno funcionamento, esses dispositivos devem ficar constantemente ligados e conectados a uma rede de *internet,* gravando o ambiente à espera de uma palavra de ativação, surgindo a dúvida se essa gravação é válida como meio de prova no processo crime. Nesses termos, por ser um meio de obtenção que viola a intimidade do usuário, tem-se uma linha tênue entre a necessidade da prova e a indispensável proteção de dados. Para tanto, a Lei n°. 13.709/2018, conhecida como Lei Geral de Proteção de Dados, disciplina por meio de normas e princípios a preservação da privacidade virtual. Nesse sentido, embora quase não utilizado no direito pátrio, para que os dados obtidos por meio de dispositivos *on-line* e assistentes virtuais sejam lícitos como prova, o usuário deve ter pleno conhecimento de sua obtenção, assim como expressamente cedê-los, se comprovado a finalidade e necessidade da prova, deverá ser cedido através da autorização judicial. Para o desenvolvimento do presente, a pesquisa bibliográfica se respaldou doutrinas, artigos, dissertações jurisprudências e textos de lei.
PALAVRAS-CHAVE: Invasão de dados; Dispositivos *on-line*; Prova no processo penal; Lei Geral de Proteção de Dados.

DATA INVASION BY ONLINE DEVICES AND VIRTUAL ASSISTANTS AND THEIR VALIDITY AS EVIDENCE IN BRAZILIAN CRIMINAL PROCEEDINGS

ABSTRACT: The objective of this study was to analyze whether the data obtained by online devices and virtual assistants, those endowed with artificial intelligence, would be valid in the Brazilian criminal procedural sphere as a means of evidence in a criminal case. Although

DOI: 10.25110/rcjs.v24i1.2021.8780

[1] Acadêmica do Curso de Direito da Unipar.

[2] Mestre em Direito. Docente do Curso de Direito da Unipar.

virtuality can be framed to the other branches of law, this paper focused on developing it in criminal proceedings, since, considering that for its full operation, those devices must be constantly on and connected to an internet network, recording the environment, just waiting for the activation word, and doubts may arise whether this recording is valid as a means of evidence in the crime process. In these terms, as a means of attainment which violates the intimacy of the user, there is a fine line between the need for evidence and the indispensable data protection. Therefore, Law No. 13.709/2018, known as the Brazilian General Data Protection Law, discipline through rules and principles the preservation of virtual privacy. In this sense, although almost not used in the national law, in order for data obtained through online devices and virtual assistants to be considered lawful as evidence, the user must have full knowledge of its collection, as well as expressly assigning them, if proven the purpose and need of the evidence, and should be transferred through judicial authorization. For the development of this study, bibliographic research was supported by doctrines, articles, jurisprudence dissertations and texts of law.
KEYWORDS: Data invasion; Online devices; Evidence in criminal proceedings; General Data Protection Law.

INVASIÓN DE DATOS POR DISPOSITIVOS EN LÍNEA Y ASISTENTES VIRTUALES Y SU VALIDEZ COMO MEDIO DE PRUEBA EN EL PROCEDIMIENTO PENAL BRASILEÑO

RESUMEN: El objetivo del presente trabajo fue analizar si los datos obtenidos por dispositivos en línea y asistentes virtuales, esos equipados con inteligencia artificial, serían válidos en el proceso penal brasileño como medio de prueba en un caso penal. Si bien la virtualidad se puede enmarcar dentro de otras ramas del derecho, se interesó en desarrollarla en el proceso penal, ya que, considerando que para su pleno funcionamiento, esos dispositivos deben estar constantemente conectados y también conectados a una red de *internet*, registrando el entorno a la espera de una palabra de activación, planteando la cuestión de si esta grabación es válida como prueba en el proceso penal. En esos términos, al ser un medio de obtención de información que atenta contra la privacidad del usuario, existe una delgada línea entre la necesidad de prueba y la protección de datos imprescindible. A tal efecto, la Ley n. 13.709 / 2018, conocida como Ley General de Protección de Datos, disciplina la preservación de la privacidad virtual a través de reglas y principios. En ese sentido, aunque poco utilizado en la legislación brasileña, para que los datos obtenidos a través de dispositivos en línea y asistentes virtuales, sean lícitos como prueba, el usuario debe ser plenamente consciente de su adquisición, así como transferirlos expresamente, si comprobado la finalidad y necesidad de prueba deberá ser transferida mediante autorización judicial. Para el desarrollo del presente, la investigación bibliográfica se apoyó en doctrinas, artículos, disertaciones de jurisprudencias y textos de derecho.
PALABRAS CLAVE: Invasión de datos; Dispositivos en línea; Prueba en proceso penal;

Ley General de Protección de Datos.

1. INTRODUÇÃO

Com o passar dos anos, a inteligência artificial ganhou notoriedade por todo o mundo e, gradualmente, ganhou espaço no cotidiano das pessoas, tanto nos lares quanto em ambientes de trabalho, isso porque se tornou uma ferramenta muito útil, pois otimiza tarefas rotineiras.

Os dispositivos dotados com essa tecnologia, como assistentes virtuais, ficam no aguardo de uma palavra chave para iniciarem uma gravação e executarem a tarefa que lhe foi dirigido.

Por esses mecanismos ficarem constantemente conectados a uma rede de internet, por meio de suas gravações, armazenam e compartilham dados com o intuito de aprimorar suas buscas e conseguir uma melhor satisfação de seu usuário.

Contudo, ao analisarmos essa informação da ótica investigativa, surge a dúvida se essa invasão de dados por assistentes virtuais ou outro dispositivo inteligente seria lícita como prova no direito processual penal brasileiro, assim como se esse cenário não seria regulado pela Lei Geral de Proteção de Dados.

Buscando a solução desse problema, depara-se com questionamentos que se os dados coletados além da finalidade do contratado entre usuário e empresa violam a privacidade do indivíduo e, consequentemente gozam de sigilosidade reflexa.

Assim, em que pese esses dados serem comuns como meio de provas em outros países, no ordenamento brasileiro é algo pouco visto e discutido diretamente.

Nesse sentido, o presente artigo propõe analisar se os dados obtidos por dispositivos *on-line* e assistentes virtuais são válidos no âmbito do processo penal brasileiro como meio de prova em um processo crime.

Também analisará a fundamentação do princípio da sigilosidade reflexa, juntamente com a Lei n°. 13.709/2018, conhecida como Lei Geral de Proteção de Dados com o intuito de averiguar sua legitimidade e licitude. Por fim, analisará qual prova essa gravação se encaixa no direito pátrio, assim como explanar sobre casos internacionais que a mesma foi útil.

2. DOS DISPOSITIVOS ONLINE E ASSISTENTES VIRTUAIS

2.1 Origem e finalidade

É sabido que vivemos em uma sociedade que está em constante evolução, consequentemente, a crescente industrialização traz consigo o avanço de diversas áreas, dentre elas, o avanço tecnológico.

A inteligência artificial, elemento essencial nos dispositivos virtuais, desde o começo surgiu com a intenção de gerar maior conforto para atividades cotidianas dos seus

usuários. Para tanto, o objetivo era criar uma máquina com capacidade de agir e pensar como um humano.

Em 1964, desenvolveu-se a "Eliza", nome dado à primeira *chatbot* do mundo e um dos primeiros sucessos da AI, esse *software* era capaz de compreender e interpretar a linguagem humana, permitindo-lhe realizar diálogos de forma automática.

Todavia, não foi um trajeto fácil e após a Segunda Guerra Mundial a inteligência artificial passou por altos e baixos, ora com e ora sem investimento científico e, principalmente financeiro, mas gradualmente essa situação modificou-se no novo milênio.

O responsável pela ascensão e desenvolvimento da AI foi o avanço da computadorização em âmbito global e, consequentemente surgiu a disponibilidade de dados de seus usuários, assim como sua colheita.

A crescente tecnológica, a partir de 2010, permitiu a inteligência artificial um aperfeiçoamento de forma surpreendente, possibilitando que essa tecnologia fosse usufruída de forma cotidiana por seus usuários. A popularização dessa se deu por meio da assistente "Siri", lançada oficialmente pela Apple em outubro de 2011.

A busca da capacidade neurológica humana levou a inteligência artificial à finalmente conseguir o feito. Um exemplo são as assistentes virtuais como a Alexa da Amazon, a Siri da Apple, a Cortana da Microsoft, até mesmo a detecção de rostos, entre outros mecanismos que se têm acesso por meio de dispositivos, como smartphones.

Destarte, essas assistentes pessoais, assim como outros dispositivos com a inteligência artificial, se tornaram ao longo dos anos e dos avanços tecnológicos grandes aliados em empresas, tarefas rotineiras, sistemas de segurança e, atualmente está ganhando espaço no direito.

2.2 Conceito e modo de funcionamento

Depois de entender-se brevemente sobre o surgimento e a finalidade da famosa inteligência artificial, é por Cozmen e Neri (2021, p. 21) sua conceituação:

> Um agente inteligente de forma geral deve ser capaz de representar conhecimento e incerteza; de raciocinar; de tomar decisões; de aprender com experiências e instruções; de se comunicar e interagir com pares e com o mundo... parece razoável se concentrar em computadores digitais cujos programas representam e raciocinam sobre conhecimento e crenças, tomam decisões e aprendem, e interagem com seu ambiente, realizando todas essas atividades ou pelo menos algumas com nível alto de sofisticação. Essa última sentença oferece uma definição ainda vaga, mas razoavelmente clara sobre o escopo da IA.

Ressalta-se que a conceituação da AI ainda é muito ingênua, devido à dificuldade

de delimitar o que seria uma conduta inteligente, visto sua relatividade dependendo do ponto de vista. Ainda, pode-se dizer que "a AI tem por objetivo implementar numa máquina a possibilidade de realizar tarefas que uma criança é capaz de realizar, mas o mais poderoso dos supercomputadores ainda não" (ROSA, 2011).

Nesse sentido, as assistentes virtuais ou dispositivos *on-line* são sistemas dotados da inteligência artificial programados para auxiliar pessoas e até mesmo empresas em tarefas cotidianas, buscando satisfazer todas as demandas possíveis de maneira direta.

Para tanto, esses mecanismos precisam estar constantemente ligados e conectados a uma rede de internet, aguardando uma palavra de ativação para exercer o comando que lhe é dirigido.

Esses dispositivos, sob o argumento de: "As empresas coletam os dados porque é muito importante saber qual o perfil daquele usuário, o que deixa ele feliz [...]" (SLEIMEN, 2019), monitoram, ouvem, gravam e arquivam o que captam no ambiente que estão inseridos.

A inteligência artificial, em assistentes pessoais, busca aprimorar suas pesquisas com base nos dados que são colhidos de seus usuários, pois, a partir do momento que aceitamos os "termos de uso" destes dispositivos, passamos a estar suscetíveis a tal violação.

O jornal Época Negócios (2019) alerta os usuários sobre o armazenamento de dados em comento:

> [...] os áudios são mandados diretamente para a nuvem. Daí, computadores tentam adivinhar a intenção do usuário e satisfazê-la. Depois, as empresas poderiam apagar a solicitação e a resposta do sistema, mas geralmente não fazem isso. A razão são os dados. Para a inteligência artificial da fala, quanto mais dados, melhor.

O que antes era guardado em disquetes, *pen drive* e CDs, hoje os dados coletados são armazenados na "nuvem" dos dispositivos, cada um possui um tempo para armazenar e após são permanentemente deletados, assim como algumas empresas permitem que os próprios usuários apaguem as informações coletadas, contudo, poucos sabem dessa possibilidade.

Observa-se que esses dispositivos trabalham com o que é funcional, por isso a necessidade de identificar as preferências de seus usuários e assim aprimorar sua funcionalidade.

Ainda, por mais que as pessoas não conheçam a extensão de seus mecanismos, ressalta-se que essa "espionagem silenciosa" não é a finalidade de uma assistente virtual ou qualquer outro dispositivo *on line,* diferente de um objeto que é comprado com a intenção de monitoramento, como uma câmera de segurança. Isto é, seu objetivo é ser um meio de informática e não um meio de investigação de seus usuários.

Ademais, os assistentes virtuais atuam de modo que possam facilitar o serviço humano, como, por exemplo, em atividades de administração e finanças o assistente

consegue produzir relatórios e planilhas, controle financeiro, transcrição, produção e revisão de textos, entre outros. Portanto, é de suma importância a utilização de dados para aprimoramento da ferramenta.

A utilização dessas informações como meio de prova é algo relativamente novo e incomum no direito brasileiro, todavia, já explorado no direto norte americano e alemão.

Desse modo, por abordar princípios invioláveis do direito pátrio, como a privacidade, acentuaram-se preocupações sobre a legalidade da utilização dos dados obtidos como prova, restando ao direito regulamentar e ditar os limites de sua utilização.

3. PRINCÍPIO DA SIGILOSIDADE REFLEXA

3.1 Princípio da não autoincriminação como base do princípio da sigilosidade reflexa

O princípio da não autoincriminação é o pilar para o princípio que será posteriormente conceituado, pois tutela o direito de que ninguém é obrigado a produzir prova contra si mesmo.

Esse princípio é previsto no inciso LXIII do artigo 5° da Constituição brasileira que se limita em dizer que o preso possui o direito de permanecer calado, sendo o direito de silêncio uma das abrangências desse princípio.

Também conhecido como *nemo tenetur se detegere,* consagra o direito de a parte não colaborar ou não fazer algo, se essas condutas são potencialmente autoincriminadoras.

Queiroz (2017, p.1) alude que o princípio em comento:

> Significa que o possível acusado de infração penal pode (livremente) colaborar ou não colaborar com a investigação, já que é sujeito de direito e não simples objeto da prova; mas, se não quiser cooperar, ninguém poderá obrigá-lo a tanto, razão pela qual, quando houver ilegal constrangimento, a confissão ou prova assim obtida será ilícita e arbitrária a eventual prisão.

Em suma, em qualquer momento do procedimento investigatório ou jus persecutório a parte não está obrigada a fazer prova contra si (SYDOW, 2021).

3.2 Conceito e finalidade no âmbito processual penal

A luz do princípio da sigilosidade reflexa tem-se que a entrega de dados obtidos em excesso, ou melhor, aqueles obtidos além da finalidade dos dispositivos *on line* ou do consentimento do titular, configura violação à sigilosidade, de modo que seria considerado nulo como prova.

O princípio em questão é instituído pelo professor Sydow (2021, p. 137):

> Por esse Princípio, dados coletados que ultrapassem a expectativa contratada pelo usuário não podem ser compartilhados com

> nenhum dos Poderes da Federação sob pena de implicar em uma autoincriminação indireta.
> Dados obtidos indiretamente por serviços informáticos prestados gozam de sigilosidade presumida e reflexa e não podem ser cedidos pelas empresas, visto que não possuem consentimento adequado dos titulares em relação à sua obtenção e seu destino. Uma vez cedidos, devem ser considerados como provas ilícitas e desconsiderados.

O professor argumenta que existe divergência entre informações transmitidas ao mundo e as divulgadas em um ambiente privado.

Veja-se que a necessidade desse princípio surge da premissa de que os dados coletados por dispositivos inteligentes não possuem clareza quando sua destinação, assim como não são expressamente cedidos por seus usuários, já que, em tese, esses não possuem conhecimento de sua obtenção.

Consoante com o exposto, Sydow (2021, p. 140) defende que se o serviço contratado possui natureza sigilosa e, se esse é quebrado sem a autorização ou conhecimento do usuário, os dados colhidos são reflexamente ilegais em seu uso para composição de autoria ou de materialidade, uma vez que violaria outro princípio, o da "Não Autoincriminação".

Todavia, com respeito ao posicionamento do brilhante professor Sydow, as finalidades dos dados obtidos são esclarecidas nos ignorados "termos de uso" do objeto adquirido, como uma assistente virtual ou qualquer outro dispositivo com inteligência artificial. Portanto, pressupõe-se que o usuário tem o conhecimento da extensão da coleta de dados, assim como as hipóteses de seu armazenamento e cessão.

Nesse sentido, o usuário não poderia alegar que não assumiu o risco por falta de conhecimento ao entregar informações ao terceiro, visto que por sua desídia ignorou os termos de uso.

Desse modo, ressalta-se que não se defende o uso indiscriminado de dados de usuários, mas sim quando a lei o exige para fins de investigação criminal ou instrução processual penal.

4. LEI GERAL DE PROTEÇÃO DE DADOS

4.1 Intuito da criação da lei

A Lei n°. 13.709/2018, conhecida como Lei Geral de Proteção de Dados, atualmente em vigor, foi inspirada no regulamento da União Europeia denominada *General Data Protection Regulation – GDPR* que possui como principal objetivo a proteção e a transparência no uso de dados pessoais.

Nos artigos 1°, *caput* e 3°, I, II e III da lei em comento discorre-se sobre seu intuito e aplicabilidade, veja-se:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> [...]
> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> I - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

A principal função da lei é disciplinar como as empresas deverão armazenar e tratar os dados dos brasileiros que lhe são confiados, para tanto, estabelece parâmentros para tal processamento.

A lei impõe limites e formas de controle sobre a cessão de dados no intuito de iniciar uma consciência informática tanto em empresas quando para as pessoas em si.

Ademais, apresenta em seu artigo 6° os princípios que norteiam a legislação:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial

> e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Ressalta-se o Princípio da Finalidade e o Princípio da Necessidade, esses, assim como o princípio da sigilosidade reflexa, discorre que o tratamento dos dados deve ser compatível com a finalidade de sua colheita previamente informado aos usuários.

Em suma, a lei obriga que empresas sejam claras quanto à finalidade da obtenção dos dados de seus usuários, evitando obtenção de informações em excesso e o controle de seu compartilhamento.

4.2 A Lei Geral de proteção de dados e o Processo Penal

Tem-se de um lado um esforço legislativo para construir uma base que garanta a proteção dos dados fornecidos e, de outro giro, temos o direito processual penal querendo utilizar esses como um novo mecanismo de comprovação de fato.

Ressalta-se LGPD regulariza a relação entre obtenção e tratamento de dados e a sua convergência com a finalidade que foi disposta e não sobre o seu uso em atividades de investigação e repressão de infrações penais.

Em seu artigo 4°, II, d é expressamente previsto:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> **III - realizado para fins exclusivos de:**
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> **d) atividades de investigação e repressão de infrações penais; ou**
> [...] (BRASIL, 2018, grifos nosso).

Todavia, ainda que não regule diretamente o uso dessas informações no direito penal, a Lei Geral de Proteção de Dados, mesmo que mínimo, o faz indiretamente.

Ao dispor que somente será permitido o tratamento de dados que estão em consenso com a finalidade de sua obtenção. Para isso, exige-se da pessoa natural ou jurídica o máximo de transparência e de determinação quanto ao seu uso, a lei evita que sejam criadas autorizações genéricas para o tratamento de tais dados.

Corrobora, nesse sentido, com o seu uso em investigações criminais, já que o pleno conhecimento da finalidade do colhimento de dados, por estar legalmente regulamentada, afasta o argumento de que é uma autorização genérica.

Todavia, sabe-se que é uma situação muito delicada, pois envolve a privacidade do cidadão, sendo que para mantê-la preservada no âmbito processual penal surgiu a iniciativa de criação da LGPD Penal.

Assim, esse anteprojeto tem o escopo de regular de forma direta o binômio entre privacidade e persecução penal, contudo, este está em fase de estudo por uma comissão de juristas, consequentemente, ainda não se encontra em vigor.

5. PROVA NO DIREITO PROCESSUAL PENAL

5.1 Conceito

Antes de considerar a assistente virtual ou outros dispositivos como meio de prova, tem-se que conceituar prova para o Processo penal.

Prova, a princípio, é tudo que auxilia no livre convencimento do juiz, em outras palavras, são os fatos e informações colhidas na investigação ou instrução processual que são apresentados ao Magistrado e ajudam a instruir sua decisão.

Embasado ao exposto, provas são os instrumentos aos quais se é possível reconstruir um fato e a sua linha cronológica, tentando demonstrar a verdade pertencente em cada caso concreto, podendo assim traçar o *iter criminis* da situação delituosa.

Nesse sentido, Capez (2014, p. 272) alude que a prova:

> Trata-se, portanto, de todo e qualquer meio de percepção empregado pelo homem com a finalidade de comprovar a verdade de uma alegação. Por outro lado, no que toca a finalidade da prova, destina-se à formação da convicção do juiz acerca dos elementos essenciais para o deslinde da causa.

Ainda, complementa Aury Lopes Jr (2016, p. 290):

> Em suma, o processo penal tem uma finalidade retrospectiva, em que, através das provas, pretende-se criar condições para a atividade recognitiva do juiz acerca de um fato passado, sendo que o saber decorrente do conhecimento desse fato legitimará o poder contido na

sentença.

Deve-se ainda considerar que a busca da prova ocorre em torno de algo, em tese, verdadeiro (NUCCI, 2020). Assim, os meios de prova compreendem tudo que possa servir, direta ou indiretamente, à demonstração da verdade que se busca no processo (CAPEZ, 2014).

Ao cerne das provas, ressalta-se que se têm tanto as lícitas, que são admitidas pelo ordenamento jurídico e as ilícitas, que não são admitidas, já que esse vai em caminho contrário aos princípios gerais do direito.

Portanto, se a prova estiver em conformidade com o ordenamento jurídico, será admissível seu uso como meio probatório em um processo ou investigação.

5.2 Prova ilícita

Em específico, tem-se que esclarecer o que é prova ilícita, ou seja, aquela que se concebe mediante uma violação das normas constitucionais ou preceitos legais, como por exemplo, uma confissão mediante tortura.

Resta claro que a prova ilegal, como o próprio nome expõe, advém de uma violação da própria lei, devendo ser desentranhada dos autos.

O momento de obtenção é fora do processo, o que a difere das provas ilegítimas, que por sua vez fere as regras do direito processual, ou seja, são adquiridas com um processo em curso, tendo como exemplo, o interrogatório do acusado realizado sem a presença do advogado, fere um disposto na lei, mas a ocorrência se dá em um momento processual.

Com a Lei 11.690/2008 tornou a prova ilícita como gênero, assim fundamenta Nucci (2020, p. 689):

> Em primeiro lugar, tomou-se como gênero a expressão provas ilícitas, do qual surgem as espécies: as obtidas em violação a normas constitucionais ou legais. Naturalmente, constituem provas ilegais as que afrontam qualquer norma da legislação ordinária, por isso, envolvem tanto as penais quanto as processuais penais. Uma prova conseguida por infração à norma penal (ex.: confissão obtida por tortura) ou alcançada violando-se norma processual penal (ex.: laudo produzido por um só perito não oficial) constitui prova ilícita e deve ser desentranhada dos autos.

Observa-se que com tal alteração, não se tem a necessidade de falar em provas ilegítimas, uma vez que ela é alcançada pela prova ilícita.

Em convergência com o exposto tem-se o entendimento do Superior Tribunal de Justiça, fundamentado pelo Ministro Sebastião Reis Junior no RHC 154093/MG (BRASIL, 2021):

> RECURSO EM HABEAS CORPUS. TRÁFICO DE DROGAS. NULIDADE. PROVA ILÍCITA. BUSCA DOMICILIAR AUTORIZADA POR TERCEIRO. AUSÊNCIA DE FUNDADAS RAZÕES PARA O INGRESSO FORÇADO DOS POLICIAIS. MANIFESTA ILEGALIDADE. 1. O art. 5º, XI, da Constituição Federal estabelece que a residência é asilo inviolável, de modo a atribuir-lhe contorno de direito fundamental vinculado à proteção da vida privada e ao direito à intimidade. Ao mesmo tempo, prevê, em numerus clausus, as respectivas exceções, quais sejam: a) se o morador consentir; b) em flagrante delito; c) em caso de desastre; d) para prestar socorro; e) durante o dia, por determinação judicial. Assim, em qualquer outra situação além das que se encontram positivadas na Carta Maior, é vedado ao agente público, sem o consentimento do morador, ingressar em sua residência, sob pena de, no campo processual, serem consideradas **ilícitas** as **provas** obtidas (AgRg no HC n. 668.957/SP, Ministro Rogerio Schietti Cruz, Sexta Turma, DJe 30/8/2021). 2. No caso, a operação policial que resultou na apreensão da droga na casa do recorrente originou-se de informação anônima passada dias antes à Polícia Militar. Os policiais, após tentativa de localização dos envolvidos, deslocaram-se até a residência de dois deles, tendo sido a busca domiciliar autorizada por terceiro - apontado como pai da coacusada, mas que não residia no imóvel. 3. Apesar da significativa quantidade de entorpecentes encontrada no imóvel do recorrente, tal descoberta não passou de mero acaso, pois não havia circunstâncias concretas que indicassem a ocorrência da prática delitiva no local. Ademais, a entrada foi permitida por terceiro que ali não residia, quando apenas ao morador da unidade habitacional caberia tal autorização. 4. Recurso em habeas corpus provido para declarar a invalidade das **provas** obtidas mediante violação domiciliar, e todas as dela decorrentes, na AP n. 5002715-89.2021.8.13.0216 e, consequentemente, para determinar a expedição de alvará de soltura em benefício do recorrente, uma vez que não houve fundadas razões nem comprovação de consentimento válido para o ingresso em seu domicílio.

Posto isso, sabe-se que no cerne as gravações ambientais há uma dificuldade em saber sua validade e aplicabilidade, sendo de suma importância ter o conhecimento sobre provas ilícitas e, assim entender que não há que se falar que gravações ambientais são meios de provas ilegais.

5.3 A licitude da gravação ambiental

5.3.1 Conceito e aplicabilidade da gravação ambiental

É notório o avanço da tecnologia, diante de tal, tem-se hoje uma facilidade de comunicação, grande parcela da população possui telefones celulares que possuem câmeras e microfone. Nota-se também que, em poder público, diversas câmeras de vigilância na cidade, localizados em semáforos, praças públicas, cruzamentos de alta intensidade e diversos outros pontos.

Não se pode confundir a interceptação ou quebra de sigilo telefônico com a gravação ambiental, por segundo ocorre comumente em locais públicos podendo ser feito sem o conhecimento dos comunicadores.

Diante disso, por se tratar de espaços públicos ou com acesso ao público, tem-se a ideia de que qualquer pessoa pode escutar a conversa dos comunicadores, afastando assim a quebra do direito à privacidade.

A diferença entre os títulos de interceptação, escuta e gravação ambiental é discorrida de forma clara pelo doutrinador Lima (2021, p. 721):

> Não se deve confundir interceptação com escuta, nem tampouco com gravação ambiental. A interceptação ocorre sem o conhecimento dos interlocutores, ou seja, nenhum deles tem consciência de que o conteúdo da comunicação está sendo captado por um terceiro; na escuta, um dos interlocutores tem conhecimento da ingerência de um terceiro na comunicação; a gravação é a captação feita diretamente por um dos comunicadores, sem a interveniência de um terceiro.

Isso posto, deve-se entender sobre a constitucionalidade da gravação ambiental em caráter clandestino, quando um comunicador tem conhecimento da gravação, sem conhecimento do outro.

O ilustre relator Ministro Cezar Peluso em seu entendimento no RE 402717/PR (BRAISL, 2009) expõe que:

> EMENTA: PROVA. Criminal. Conversa telefônica. Gravação clandestina, feita por um dos interlocutores, sem conhecimento do outro. Juntada da transcrição em inquérito policial, onde o interlocutor requerente era investigado ou tido por suspeito. Admissibilidade. Fonte lícita de prova. Inexistência de interceptação, objeto de vedação constitucional. Ausência de causa legal de sigilo ou de reserva da conversação. Meio, ademais, de prova da alegada inocência de quem a gravou. Improvimento ao recurso. Inexistência de ofensa ao art. 5º, incs. X, XII e LVI, da CF. Precedentes. Como gravação meramente clandestina, que se não confunde com interceptação, objeto de vedação constitucional, é lícita a prova consistente no teor de

> gravação de conversa telefônica realizada por um dos interlocutores, sem conhecimento do outro, se não há causa legal específica de sigilo nem de reserva da conversação, sobretudo quando se predestine a fazer prova, em juízo ou inquérito, a favor de quem a gravou.

Percebe-se que não ocorre a ofensa ao artigo 5º, inciso X, XII e LVI da Carta Magna, sendo lícita a prova adquirida deste modo. Ao atrelar o assistente virtual ao entendimento, se torna perfeitamente capaz da prova produzida por meio da gravação ser válida. Nessas circunstâncias, há conhecimento da parte que adquire o produto, ao concordar com os termos de uso do dispositivo *on line,* tem a ciência que o fabricante do produto armazene os dados coletados em uma nuvem.

Como exemplo, a Alexa, assistente virtual da Amazon, permite que as interações com os mecanismos sejam armazenadas na nuvem. Veja-se um trecho do contrato que deixa de forma clara o armazenamento dos dados: "Quando você fala com a Alexa, uma gravação do que você solicitou é enviada à nuvem da Amazon para que os nossos sistemas de reconhecimento de fala e compreensão da linguagem natural possam processar e responder à sua solicitação" (AMAZON, 2021, *on line*).

O código de proteção da Amazon (2021, *on line*) e de terceiros é objetivo a afirmar que as informações pessoais podem ser fornecidas em diversos casos, como se pode ver:

> Proteção da Amazon e de terceiros: Nós fornecemos informações sobre contas e outras informações pessoais quando acreditamos que esse fornecimento é adequado para fins de cumprimento com a lei; de execução ou aplicação de nossas Condições de Uso e outros acordos; ou de proteção dos direitos, bens e segurança da Amazon, de nossos usuários ou de terceiros.

É mister, o conhecimento da parte adquirente ao produto que faz gravações, quando solicitado e armazena na nuvem, podendo ser utilizado posteriormente.

Em contrapartida, é um meio de prova não utilizado e não previsto no ordenamento jurídico atual, mas se aplica de forma análoga ao entendimento do Supremo Tribunal Federal, não tendo o que se falar em inconstitucionalidade na utilização desse meio de prova por ser considerada uma gravação ambiental.

Firmando novamente seu entendimento tem-se mais um brilhante acerto por parte do relator Ministro Cezar Peluso, no RE 583937 QO-RG/RJ (BRASIL, 2009), que discorre:

> EMENTA: AÇÃO PENAL. Prova. Gravação ambiental. Realização por um dos interlocutores sem conhecimento do outro. Validade. Jurisprudência reafirmada. Repercussão geral reconhecida. Recurso extraordinário provido. Aplicação do art. 543-B, § 3º, do CPC. É lícita a prova consistente em gravação ambiental realizada por um dos interlocutores sem conhecimento do outro.

De igual pensamento o relator Ministro Joaquim Barbosa no AI 560223 AgR/SP (BRASIL, 2011), abrilhanta que:

> EMENTA: AGRAVO REGIMENTAL EM AGRAVO DE INSTRUMENTO. GRAVAÇÃO AMBIENTAL FEITA POR UM INTERLOCUTOR SEM CONHECIMENTO DOS OUTROS: CONSTITUCIONALIDADE. AUSENTE CAUSA LEGAL DE SIGILO DO CONTEÚDO DO DIÁLOGO. PRECEDENTES. 1. A gravação ambiental meramente clandestina, realizada por um dos interlocutores, não se confunde com a interceptação, objeto cláusula constitucional de reserva de jurisdição. 2. É lícita a prova consistente em gravação de conversa telefônica realizada por um dos interlocutores, sem conhecimento do outro, se não há causa legal específica de sigilo nem de reserva da conversação. Precedentes. 3. Agravo regimental desprovido.

Em mesmo sentido, países como, Estados Unidos e Alemanha, no Tribunal Regional de Regensburg apresentam casos em que os assistentes virtuais atuaram como meios de provas, podendo assim chegar ao agente que praticou o delito.

O equipamento em questão funciona por meio de ativação por palavra-chave, gravando apenas trechos de áudio não capitando uma conversa privada inteira.

É um caminho onde se podem ter provas concretas em casos de violência doméstica, como por exemplo, podendo colocar a palavra de ativação de forma discreta, em que o agressor não saberá que está sendo gravado, assim se enquadrando perfeitamente nos casos defendidos pelo Supremo Tribunal Federal.

Destarte, a invasão de dados por dispositivos dotados com inteligência artificial pode ser considerada válida no âmbito de um processo crime, por ser considerada uma gravação ambiental, logo pode ser tanto cedido pela parte ou requerido pelo juiz à empresa, devendo esta ceder as informações e notificar seu usuário sobre o uso do mesmo.

5.4 Aplicabilidade de assistentes virtuais e dispositivos online como meio de prova em outros países

Finda a apresentação teórica e com a ideia que é devidamente aceitável que o assistente virtual como meio de prova é de suma importância, visto que, hoje grandes parcelas da sociedade possuem *smartphones*, *Alexa, Google Assistent*, entre outros dispositivos inteligentes.

Oportunamente cabe ressaltar os casos criminosos que tiverem uma participação de tal tecnologia para ajudar os investigadores a solucionar o caso, mediante provas advindas dos assistentes virtuais, gravação ambiental e mesmo o rastreamento de seu aparelho.

A priori, tem-se o caso de Silvia Galva, moradora do estado da Flórida nos Estados Unidos, o presente caso tem uma particularidade, pois, ela foi encontrada morta com uma

lâmina em seu peito, o principal suspeito Adam Crespo, namorado da vítima, afirmou que ocorreu uma briga, porém, não há testemunhas para confirmar o que de fato aconteceu.

As investigações policiais nesse caso se deparam então com a possibilidade da assistente virtual, Alexa, sistema da Amazon, servir como uma testemunha, pois, acredita-se que na base de dados gravados podem ter trechos da discussão do casal, assim podendo contribuir de forma fundamental para a resolução do caso.

Observa-se que em casos onde não se têm testemunha a tentativa de colher informações armazenadas em dispositivos inteligentes é de relevância, uma vez que pode contribuir com dados até então impossíveis de serem produzidas.

A aplicabilidade do caso no Brasil seria possível, tendo em vista que o proprietário do dispositivo tem o conhecimento da capacidade de gravação, sendo expressamente aceito ao concordar com os termos de uso do aparelho, sendo afastada a ideia de uma escuta não autorizada previamente pela autoridade judicial.

Outro caso notório é o do Robert Durst, que durante a gravação de um documentário que tratava a respeito de sua ligação com três mortes, sendo negado de forma assídua pelo por ele, porém, ao ir ao banheiro ainda com o microfone ligado confessou ambos os crimes. O material tido como gravação ambiental foi fornecido e aceito pelas autoridades policiais, a partir do qual se pode condenar o acusado.

Em mesmo cerne, a aplicação análoga ao caso de Robert Durst é perfeitamente possível, já que a gravação ambiental clandestina, como já discorrida, se aplica perfeitamente ao caso em comento. Ciente de que seu áudio está sendo gravado e ainda assim, confessa o crime, é possível, em detrimento da não necessidade de autorização judicial para realizar tal ato.

Com base nos casos e sua aplicação em outros países, a evolução da tecnologia vem como um meio de auxiliar de todas as formas, atuando como importante meio de prova, já que a gravação de vídeo e áudios ocorre de forma instantânea ao olhar dos jovens que estão conectados a todo momento.

A Lei Brasileira está tomando forma e navegando em direção a essa nova modalidade de prova, devendo ser regulamentada e aplicada.

6. CONCLUSÃO

Ao compreender-se a evolução dos dispositivos dotados de inteligência artificial, assim como sua forma de funcionamento, colheita e armazenamento de dados, percebe-se a sua utilidade como meio de prova no processo penal brasileiro.

Por mais que a sua finalidade seja como meio de informática e não como de prova, observa-se a previsão, nos termos de uso desses mecanismos inteligentes, que se a lei exigir será disponibilizado os dados do usuário quando tratar de investigação ou processo crime.

De outro ponto, o princípio da sigilosidade defende que a disposição de dados além da sua finalidade seria uma conduta ilegal, visto que viola o direto à inviolabilidade

dos usuários e, potencialmente, infringir o princípio da não autoincriminação, contudo, o brilhante princípio encontra alguns óbices.

Os termos de compartilhamento de dados, em caso em situações de investigação criminal, são consentidos pelos usuários, tornando, por mais que delicada, uma prova cabível no ordenamento jurídico pátrio, se assim pré-estabelecido.

Ademais, a Lei n°. 13.709/2018, conhecida como Lei Geral de Proteção de Dados, apesar de não disciplinar sobre atividades de investigação e repressão de infrações penais, normatiza sobre a clareza que, as empresas e pessoas físicas, devem ter ao tratar de dados de seus usuários. Além disso, disciplinam como não ultrapassar da finalidade pretendida, o que de forma indireta ajuda afastando o argumento de ser uma autorização genérica.

Na questão de provas, ressalta-se que as informações colhidas por dispositivos inteligentes são gravações do ambiente do qual se encontram inseridas, isto é, não passa de uma gravação ambiental.

Contudo, ao considerá-las como meio de prova, apesar de lícita, não deixa de ser uma medida de obtenção invasiva não só para com o usuário, mas também com terceiros que se relacionaram, por isso a problemática em seu redor.

Conclui-se, por derradeiro, que os dados obtidos por meio de dispositivos *on-line* e assistentes virtuais, são lícitos como meio de prova no âmbito processual penal brasileiro. Para tanto, o usuário deve ter conhecimento de sua obtenção, podendo esse ceder voluntariamente ou, se comprovado a finalidade e necessidade da prova, não possuindo outro meio para obtê-la, o juiz de forma fundamentada poderá requisitar.

REFERÊNCIAS

ALEXA vira ‘testemunha’ em caso de morte nos EUA. **Olhar digital**, 04 nov. 2019. Disponível em: https://olhardigital.com.br/2019/11/04/noticias/alexa-vira-testemunha-em-caso-de-morte-nos-eua/. Acesso em: 28 nov. 2021.

ALEXA, dispositivo echo e sua privacidade. **Amazon**. Disponível em: https://www.amazon.com.br/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V. Acesso em: 17 out. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 out. 2021.

BRASIL. **Lei nº 13.709/2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 154093/MG**. Relator Sebastião Reis Júnior. 19 out. 2021. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202102989984&dt_publicacao=19/10/2021. Acesso em: 16 out. 2021.

BRASIL. Supremo Tribunal Federal. **Agravo de Instrumento nº 560223/SP**. Relator Joaquim Barbosa. 29 abr. 2011. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur191446/false. Acesso em: 16 out. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 402717/PR**. Relator Cezar Peluso. 13 jan. 2009. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur87079/false. Acesso em: 16 out. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 583937/RJ**. Relator Cezar Peluso. 18 dez. 2009. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral1282/false. Acesso em: 16 out. 2021.

BRUNATO, Ingredi. **Como uma assistente virtual se tornou testemunha de uma investigação de assassinato**. Aventuras na História, 01 nov. 2020. Disponível em: https://aventurasnahistoria.uol.com.br/noticias/reportagem/como-uma-assistente-virtual-se-tornou-testemunha-de-uma-investigacao-de-assassinato.phtml. Acesso em: 28 out. 2021.

CANTO, Gisele Belo. **Resumo das provas no direito processual penal para a PF e PRF**. Estratégia, 13 fev. 2021. Disponível em: https://www.estrategiaconcursos.com.br/blog/provas-direito-processual-penal-pf-prf/. Acesso em: 25 out. 2021.

CAPEZ, Fernando. **Curso de processo penal**. 21. ed. São Paulo: Saraiva, 2014.

COZMAN, Fabio G.; PLONSKI, Guilherme Ary; NERI, Hugo. **Inteligência artificial**: avanços e tendência. São Paulo: Instituto de Estudos Avançados, 2021. Acesso em: 05 jun. 2021.

CUIDADO: seus dispositivos ouvem, gravam e arquivam o que você fala. **Época Negócios**. 20 maio 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/05/cuidado-seus-dispositivos-ouvem-gravam-e-arquivam-o-que-voce-fala.html. Acesso em: 05 jun. 2021.

EBERHARDT, Marcos. **Com a palavra... Alexa?** 31 mar. 2021. Disponível em: https://marcoseberhardt.com.br/conteudos/com-a-palavra-alexa/. Acesso em: 17 out. 2021.

HISTÓRIA da inteligência artificial. **X2 Inteligência Digital**. 20 fev. 2020. Disponível

em: https://x2inteligencia.digital/2020/02/20/historia-da-inteligencia-artificial/. Acesso em: 05 jun. 2021.

LAVAGNOLI, Silvia. Como surgiu a inteligência artificial? **Opencadd**, 31 jan. 2019. Disponível em: https://opencadd.com.br/como-surgiu-a-inteligencia-artificial/. Acesso em: 05 jun. 2021.

LIMA, Renato Brasileiro de. **Manual de processo penal**. 9. ed. Salvador: JusPodivm, 2021.

LOPES JUNIOR, Aury. **Direito processual penal**. 13. ed. São Paulo: Saraiva. 2016.

MILIONÁRIO é detido por gravação na qual confessa assassinatos. **Jornal de Beltrão,** 16 mar. 2015. Disponível em: https://www.jornaldebeltrao.com.br/noticia/217893/milionario-e-detido-por-gravacao-na-qual-confessa-assassinatos. Acesso em: 28 out. 2021.

NOTIFICAÇÃO de privacidade da Amazon. **Amazon**. 14. ago. 2020. Disponível em: https://www.amazon.com.br/gp/help/customer/display.html?nodeId=201909010. Acesso em: 17 out. 2021.

NUCCI, Guilherme de Souza. **Curso de direito processual penal**. 17. ed. Rio de Janeiro: Forense, 2020.

QUEIROZ, Paulo. **Princípio da não autoincriminação.** 17 mar. 2017. Disponível em: https://www.pauloqueiroz.net/principio-da-nao-autoincriminacao/. Acesso em: 20 out. 2021.

ROSA, João Luís Garcia. **Fundamentos da inteligência artificial**. Rio de Janeiro: LTC, 2011.

SAMPAIO. Alexandre Santos. **Gravação ambiental após o pacote anticrime**. 01 mar. 2021. Disponível em: https://jus.com.br/artigos/89135/gravacao-ambiental-apos-o-pacote-anticrime. Acesso em: 17 out. 2021.

SÉRVIO, Gabriel. **Olhar digital**. 01 nov. 2020. Disponível em: https://olhardigital.com.br/2020/10/24/noticias/como-surgiram-e-quais-sao-os-principais-assistentes-inteligentes/. Acesso em: 05 jun. 2021.

SLEIMEN, Cristina. Invasão de privacidade no celular: ele está te ouvindo? **Dialogando Vivo**, 12 set. 2019. Disponível em: encurtador.com.br/eikK6. Acesso em: 23 jun. 2021.

SYDOW, Spencer Toth. **Da necessária relativização do elemento informático perante o princípio da manipulação**. 25 ago. 2019. Disponível em: https://s3.meusitejuridico.com.br/2019/08/7913457e-relativizacao-elemento-informatico-principio-manipulabilidade.pdf. Acesso em: 01 out. 2021.

SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. 2. ed. Salvador: Editora JusPodivm, 2021.