UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

LAURA RODRIGUES RORIZ

OS LIMITES DA VIGILÂNCIA ESTATAL IMPOSTOS PELA PRIVACIDADE: O caso do sistema Pegasus

Brasília

2022

Autora: Laura Rodrigues Roriz

OS LIMITES DA VIGILÂNCIA ESTATAL IMPOSTOS PELA PRIVACIDADE: O caso do sistema Pegasus

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.
Orientador: Angelo Gamba Prata de Carvalho.

Brasília
2022

LAURA RODRIGUES RORIZ

OS LIMITES DA VIGILÂNCIA ESTATAL IMPOSTOS PELA PRIVACIDADE: O caso do sistema Pegasus

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília.

BANCA EXAMINADORA

_____

Prof. Angelo Gamba Prata de Carvalho (Orientador - UnB)

_____

Prof. Dr. Wilson Roberto Theodoro Filho, (Avaliador – UnB)

_____

Prof. Dra. Fernanda de Carvalho Lage (Avaliadora – UnB)

Brasília

2022

AGRADECIMENTOS

A experiência como graduanda em direito pela Universidade de Brasília não pode ser resumida de melhor forma senão como a plena confirmação de que a vida humana é, essencialmente, uma experiência compartilhada.

Destarte, reservo este espaço do trabalho para desafiar-me a transladar ao papel a minha gratidão à infinidade de afeto e respeito que continuamente vivencio, como uma audaciosa tentativa de demonstrar tamanho orgulho e o júbilo que sinto por ter seres tão extraordinários ao meu redor.

A cada pedacinho de amor que tive o prazer de conhecer, seguem minhas gratulações.

Meus primevos agradecimentos destinam-se aos meus pais, os quais abdicaram de parte de si para serem o melhor que poderiam para mim. À minha mãe, Polyana de Fátima Roriz, que demonstra seu amor na sutileza dos gestos diários, proporcionando-me o conforto, o cuidado e o amparo basilares para o cumprimento de minha formação acadêmica. Igualmente, ao meu pai, José Gustavo Lopes Roriz, cuja existência inspira e encanta unanimemente todos aqueles que o conhecem, figurando como um cativante exemplo de complacência, carinho e responsabilidade. Orgulho-me imensamente daqueles que me concederam o regozijo que é viver.

Agradeço à minha avó, Maria de Fátima Tormin Roriz, que indubitavelmente é a verdadeira expressão do mais puro amor e ternura que já tive o prazer de me deparar. Estar em sua presença causa-me a fascinante antítese de me fazer questionar como pude merecer tê-la como minha segunda mãe, mas, ao mesmo tempo, faz-me crer que tudo posso. É inexplicável a nossa ligação, a maneira como teu olhar me acalma e o apoio que tuas palavras me proporcionaram para que eu chegasse até aqui.

Meus mais sinceros agradecimentos também à família que escolhi cultivar, aquela que adentrou em minha vida para alegrá-la e engrandecê-la. Refiro-me aos meus amigos, sopros de leveza em meio à dinamicidade e às incertezas que marcam essa fase inicial da vida adulta.

Amizade é escolher compartilhar a sua vida com aqueles que, inicialmente, são completos desconhecidos, mas que, por meio das trocas de conversas, de momentos e de companheirismo, acabam por tornar-se parte insubstituível de nossas vidas. Amizade é escolher acolher, e eu me sinto plenamente abraçada por vocês, meus amigos. Obrigada por tanto!

Como diria Vinícius de Moraes, "*a amizade além de contagiosa é totalmente incurável*", afinal, os verdadeiros amigos permanecem incuravelmente marcados em nossos corações, independente do rumo que nossas vidas venham a nos levar.

Não poderia deixar de dedicar meus agradecimentos também ao meu orientador, Angelo Gamba Prata de Carvalho, grande referência tanto como notável profissional, quanto como ser humano. Sua disposição única para auxiliar-me na elaboração da presente monografia, mesmo diante de algumas dificuldades, foi imprescindível para que tudo desse certo.

Enfim, a todos aqueles que contribuíram, direta ou indiretamente, para o desenvolvimento deste trabalho de pesquisa, cujas companhias afloraram num contínuo compartilhamento de alegrias, aprendizado e enriquecimento: meu muito obrigada!

“Não serei o poeta de um mundo caduco. Também não cantarei o mundo futuro.
Estou preso à vida e olho meus companheiros. (...)
O tempo é a minha matéria, do tempo presente, os homens presentes, a vida presente.”

Carlos Drummond de Andrade

RESUMO

O propósito desta pesquisa concerne em estruturar uma análise crítica acerca dos limites da vigilância estatal frente aos direitos constitucionais à privacidade e à proteção de dados pessoais. Com o escopo de realizar esse contraponto da atuação do Estado frente aos referidos direitos fundamentais, o presente trabalho se vale de um caso prático que repercutiu a nível internacional, referente à utilização, por parte de entidades estatais, do sistema Pegasus, um *software* malicioso capaz de acessar toda a atividade de qualquer aparelho celular sem que haja qualquer tipo de consentimento do titular. Ora, quais são os limites da atuação estatal, no que tange aos meios utilizados para provimento da segurança pública? Tal questionamento é examinado na presente monografia, na qual são trabalhados alguns conceitos basilares ao entendimento da sistemática de proteção à privacidade, para aplicá-los à realidade prática e, assim, melhor visualizar as possíveis respostas para a supramencionada pergunta.

PALAVRAS-CHAVE: Proteção de dados; Sistema Pegasus; Vigilância estatal; Privacidade.

ABSTRACT

The purpose of this research is structuring an analysis of the limits of state surveillance face of constitutional rights to privacy and protection of personal data. With the aim of carrying out this practical work at all fundamental points, the present paper makes use of a practical case, about the Pegasus spyware, a malicious software used by state entities capable of accessing all the activity of any mobile device without any type of consent. Now, what are the limits of state action, in terms of the means used to provide public security? That question is examined at this monography in a practical context and, using that to understand better the privacy hypotheses for the above-mentioned question.

KEYWORDS: Data Protection; Pegasus spyware; State surveillance; Privacy.

LISTA DE ABREVIATURAS E SIGLAS

ADI - Ação Direta de Inconstitucionalidade

AIC - Agência de Inteligência Criminal Mexicana

AI - Inteligência Artificial

BND - Departamento Federal de Investigações da Alemanha

CC - Código Civil

CF - Constituição Federal de 1988

GDPR - Regulamento Geral de Proteção de Dados da União Europeia

IBGE - Instituto Brasileiro de Geografia e Estatística

SISP - Sistema de Administração dos Recursos de Tecnologia da Informação

LAI - Lei de Acesso à Informação, Lei n. 12.527/2011.

LGPD - Lei Geral de Proteção de Dados, Lei n. 13.709/2018

MP - Medida Provisória

TST – Tribunal Superior do Trabalho

SMP - Serviço Móvel Pessoal

STF - Supremo Tribunal Federal

STFC - Serviço Telefônico Fixo Comutado

SUMÁRIO

INTRODUÇÃO

Desde os primórdios das discussões acadêmicas acerca do direito à privacidade, a evolução tecnológica estava evidentemente muito associada à questão das informações pessoais, bem como aos riscos que o fluxo de dados poderia gerar à privacidade e à autodeterminação de cada indivíduo.

Atualmente, verifica-se uma tendência de ampliação global em relação à criação de legislações firmes sobre proteção de dados, até como uma forma de os países obterem melhor inserção no mercado global, afinal, o fluxo de informações de alguns países já se encontra num patamar de exigências protetivas que não havia antigamente.

Contudo, para além dessa motivação mercadológica, os Estados precisam pensar num sistema de proteção à privacidade, à intimidade e aos dados pessoais também sob a perspectiva da sua própria atuação interna, de vigilância e segurança nacionais.

Isso porque, os recursos tecnológicos - que são cada vez mais intrínsecos à sociedade atual e influem incessantemente na vida profissional, social, política e pessoal dos indivíduos - foram naturalmente incorporados à atuação da máquina estatal, a qual utiliza-se de determinadas tecnologias para imprimir celeridade e eficiência às suas atividades internas.

Ora, não se pode olvidar que o Estado figura como o maior agente gerador e concentrador de dados pessoais, haja vista necessitar da coleta destes para a execução das políticas públicas, para execução de atividades relacionadas ao pagamento de salários, para gestão de servidores públicos, bem como por conta da prestação de sua função jurisdicional.

Assim, dada a magnitude das bases de dados estatais e a intensificação do uso de vias digitais para seu processamento, o tratamento de dados por parte dos entes estatais, se feito de maneira inadequada, pode reverberar em efeitos extremamente prejudiciais aos indivíduos.

Como exemplo, considerando o enorme volume de dados que o Estado geralmente colhe em suas pesquisas, qualquer vazamento de dados acaba por vulnerabilizar centenas de milhares de cidadãos. Ou, o uso de ferramentas de inteligência artificial cujos algoritmos estejam eivados de critérios discriminatórios, pode gerar lesões de direito inimagináveis aos grupos discriminados.

Outro exemplo de risco aos direitos fundamentais dos indivíduos que pode ser causado pela atuação indevida do Estado refere-se ao uso de ferramentas de vigilância estatal que violem o direito à privacidade, bem como os princípios de proteção de dados.

A presente monografia pretende abordar essa última situação, com enfoque na atividade de vigilância do poder público. Para tanto, são feitas considerações iniciais acerca de elementos importantes para a compreensão da sistemática de proteção de dados, como a origem do direito à privacidade e a mudança de paradigma do direito civil para que se pudesse abarcar os direitos extrapatrimoniais. Além disso, explica-se o que efetivamente são dados e algumas de suas classificações, como a de dados sensíveis.

Em seguida, o presente trabalho contextualiza todos esses conceitos à realidade prática, demonstrando o quão importante é a discussão e a efetivação da proteção à privacidade e aos dados pessoais, principalmente em um contexto de intenso fluxo informacional.

Logo após, esta monografia aborda sobre exemplos de atuação do Estado nas quais a utilização de dados pessoais é pressuposto indispensável, para, só então, entrar na perspectiva focada no caso do sistema Pegasus. Nessa ocasião, é realizada uma profunda descrição do referido *software*, bem como de toda a polêmica gerada por ele e suas implicações na realidade prática.

Feito isso, parte-se para o âmbito de incidência e bases legais que a Administração Pública deve se atentar para a realização de atividades que abarquem a utilização de dados pessoais. Neste ponto, vale mencionar que a LGPD adota um método principiológico – logo, muitas das normas são abstratas -, isso significa que a sua concretização necessita de bastante sopesamento e profunda clareza do espírito da norma de proteção de dados.

Assim, cada princípio elencado pela Lei Geral de Proteção de Dados será abordado frente ao caso Pegasus, no intuito de melhor entender o grau de desacordo que o referido sistema tem em relação à sistemática de proteção de dados.

Após, tratar-se-á acerca de um dos mais consideráveis conflitos do poder público, referente à tensão dos princípios do direito administrativo em face do direito à privacidade, com enfoque nos preceitos de publicidade, de supremacia do interesse público, de eficiência e da transparência.

São constantes os confrontos entre os princípios da Administração Pública com o direito à privacidade e à proteção de dados, contudo, o ordenamento precisa encontrar um ponto de equilíbrio e coesão capazes de nortear a atuação dos entes públicos sem ferir aos direitos da personalidade.

CAPÍTULO 1 – Direitos à privacidade e à proteção de dados pessoais - importância na sociedade atual

1.1. Direito à privacidade

O direito civil ocidental possui sua formação nitidamente marcada pela proteção a direitos relativos à propriedade e, por muito tempo, a atuação jurisdicional pautou-se quase exclusivamente na proteção de direitos referentes a coisas tangíveis/patrimoniais.

Contudo, com o passar das evoluções sociais, especialmente com a progressão das inovações tecnológicas, começaram a surgir algumas preocupações que iam além do mundo tangível, momento no qual passou-se a discutir acerca das garantias do indivíduo, como pessoa detentora de direitos não necessariamente ligados às suas posses, mas à sua própria individualidade.

Pois bem. O início das reflexões alusivas ao direito à privacidade está intimamente ligado ao fortalecimento dos direitos individuais[1], oportunidade na qual há um afastamento da ideia de proteção voltada à propriedade, para que a sociedade passasse a considerar a necessidade de uma proteção conectada a um *direito da personalidade*.

Passo seguinte, desenvolveu-se a concepção de que existe uma esfera da vida/personalidade das pessoas que é intransponível, isto é, que nem o Estado e nem as pessoas podem violar. Essa esfera se refere à *intimidade*; um âmbito inviolável e que ninguém poderia ultrapassar.

Neste ponto, é necessário mencionar que a academia teve fundamental importância para que ocorresse essa mudança de ideias e concepções, contribuindo enormemente para o fortalecimento do direito à privacidade.

Um importante marco para o início das reflexões voltadas para a privacidade refere-se ao artigo "*The Right to Privacy*", publicado em 1890, na *Havard Law Reveiw*, por Samuel Warren e Louis Brandeis.

---

[1] O caso *Olmstead v. United States* é um marco na para a mudança de entendimento acerca dos direitos civis, a fim de que se afirmasse a necessidade de proteção dos direitos da personalidade. A relevância jurídica está no voto do Membro da Suprema Corte, Louis Brandeis, que ora se transcreve: *They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. Louis Brandeis, então juiz da Suprema Corte norte-americana, em sua opinião divergente* (*dissent*, 277 U.S. 438).

A referida obra trata-se de uma análise acerca do desafio a ser enfrentado pelo direito em meio às evoluções tecnológicas, de modo a colocar em destaque a necessidade da proteção à intimidade dos indivíduos. Muito provavelmente não se sabia, à época, a proporção que as tecnologias tomariam, nem mesmo a maneira como nossos dados estariam em profusão, mas já se iniciava uma preocupação com o poder que a informação poderia ter e nos impactos que o indivíduo poderia sofrer em relação a isso.

É interessante observar que é justamente a evolução tecnológica que escancara a necessidade de discutir a proteção da vida privada. Destarte, todo debate de privacidade sempre esteve muito ligado aos desafios que a tecnologia impõe ao direito, afinal, os mais cômodos espaços podem ser violados por meio dessas tecnologias.

Inclusive, se verificarmos as regiões do globo pioneiras na formalização legal de sistemas de proteção de dados, quais sejam Europa e Estados Unidos, isso se deu muito provavelmente em consonância justamente com o fato de serem também localidades nas quais o desenvolvimento econômico e tecnológico ocorreram mais cedo[2], em comparativo com as demais regiões.

Fato é, que o mencionado artigo quebrou diversos paradigmas quanto ao entendimento jurídico que se tinha sobre a esfera privada, fazendo um comparativo crítico extremamente importante para a época, com relação ao direito à propriedade e ao direito à privacidade.

Inobstante a vultosa notoriedade do trabalho de Warren e Brandeis, é importante mencionar que eles não delimitaram em seu texto um conceito fechado do que seria o *right to privacy*, de modo que seu trabalho tem um cunho muito doutrinário e teórico no sentido de simplesmente demonstrar a importância da proteção à privacidade como um direito intrínseco ao indivíduo e não como algo voltado à propriedade ou a patentes, por exemplo.

Segundo eles, "*a proteção da sociedade deve vir principalmente a partir do reconhecimento dos direitos do indivíduo. Cada homem é responsável pelos seus próprios atos e omissões, unicamente*"[3](tradução livre).

---

[2] "Essa origem está ligada a uma série de fatores, desde o fato de que um desenvolvimento econômico e tecnológico mais cedo e mais intenso nessas regiões proporcionou condições para que problemas especificamente ligados à privacidade e a dados pessoais fossem levados em consideração antes e, a partir daí, fossem estabelecidos instrumentos regulatórios e jurídicos de tutela às liberdades individuais afetadas, incluindo o direito à privacidade". DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p.23.

[3] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890.

A partir dessas novas concepções, os acadêmicos e operadores do direito passaram a levantar questões relativas ao chamado "*right to be let alone*", ou direito de ser deixado em paz, em tradução literal, referindo-se a uma postura negativa do Estado.

Tal entendimento está bastante ligado à noção de *volenti non fit iniuria*[4], isto é, se houve um ato de vontade e consentimento, não há violação de direito. Em contrapartida, em casos nos quais há alguma decisão judicial que determine a exposição de determinados dados, possivelmente não mais imperaria a privacidade.

A partir disso, despontaram na jurisprudência alguns posicionamentos inovadores, como o emblemático *dissent* (voto divergente) do julgamento *Olmstead v. United States*, de 1928, que, apesar de ter sido voto vencido, ainda hoje é lembrado como um parecer paradigmático de aplicação da Quarta Emenda Americana[5] diante de ameaças tecnológicas.

O referido voto menciona a exigência de mandado judicial para atos de vigilância estatal realizados por meios eletrônicos, de modo a evidenciar a necessidade de preocupação do Estado quanto à privacidade dos cidadãos, para além de violações físicas à pessoa ou ao direito de propriedade.

Trata-se de um marco da significativa mudança no entendimento da Corte Norte-americana acerca da proteção à privacidade face à atividade de investigação estatal. Conforme leciona Daniel Pesciotta, tal precedente influenciou decisões de tribunais estaduais americanos, bem como contribuiu para que legisladores providenciassem adaptações importantes em leis que versavam sobre escuta e gravação telefônica. Tudo isso sem contar a representatividade que o caso teve na discussão acerca da disputa entre os direitos referentes às liberdades individuais e o anseio por uma maior efetividade da aplicação da lei penal[6].

---

[4] Expressão em latim que significa, em tradução literal: "nenhuma injustiça se comete a quem agiu voluntariamente". Essa ideia é oponível, quando se entende que o Estado jurisdicional não interfira em situações que foram acordadas e plenamente consentidas entre os indivíduos.

[5] A quarta emenda americana possui a seguinte redação: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*., cuja tradução para o português refere-se ao seguinte: "O direito das pessoas de estarem seguras em suas pessoas, casas, papéis e pertences, contra buscas e apreensões não razoáveis, não deve ser violado e nenhum mandado deve ser emitido, mas por causa provável, apoiado por juramento ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas" (tradução livre).

[6] PESCIOTTA, Daniel. I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century. Case Western Reserve Law Review, Vol. 63, Issue 1 (Fall 2012), pp. 245-247.

Não obstante o início da profusão de estudos e posicionamentos em prol do direito à privacidade, ainda levou considerável tempo para que houvesse previsão legislativa do direito à personalidade, principalmente se considerarmos os ordenamentos de *civil law*.

Os legisladores dos Códigos Civis clássicos se recusaram a trazer os referidos direitos, mantendo a concepção de propriedade como norteadora do direito civilista. Uma das explicações para isso é que havia uma preocupação material muito forte nos códigos da época, os quais possuíam um caráter essencialmente burguês e, portanto, preocupavam-se com toda a matéria que estivesse relacionada com a circulação de riquezas.

Consequentemente, os ramos jurídicos elencados diziam respeito, basicamente, ao direito dos contratos (seara jurídica cujo objeto figura-se como um meio que vai de circulação da propriedade), ao direito das sucessões (que regula o meio pelo qual a propriedade será transmitida pelas gerações) e aos direitos de propriedade, de maneira geral.

Quanto ao ordenamento pátrio, o primeiro Código Civil (CC) a contemplar disposições acerca dos direitos de personalidade é o atual (Lei n. 10.406/2022)[7], o qual define, em seu artigo 11, que "*com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária*".

Tal previsão surge como uma decorrência lógica do princípio da dignidade da pessoa humana, que fora reconhecido como fundamento da República Federativa do Brasil, em seu art. 1º, inciso II [8].

A propósito, a Constituição Federal de 1988 foi além e trouxe em sua redação a previsão ao direito à privacidade como uma garantia fundamental do indivíduo, dispondo em seu art. 5º, inciso X que "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*.

Neste espeque, uma vez reconhecido o direito à privacidade - que se refere à proteção da vida privada do indivíduo, como uma prerrogativa intrínseca à personalidade

[7] Os direitos da personalidade estão elencados no Código Civil em capítulo próprio, compreendido entre os artigos 11 e 21.

[8] Constituição Federal, artigo 1º: "A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: III - a dignidade da pessoa humana".

dos indivíduos e que deve ser intangível e inviolável -, essencial que façamos uma reflexão acerca da eficácia material desta previsão constitucional.

1.2. O que são dados pessoais?

Preliminarmente, interessante abordar uma diferenciação basilar, no que tange aos conceitos de dado e de informação. Segundo Danilo Doneda, dado pode ser entendido como uma espécie de "pré-informação", anterior à interpretação, enquanto a informação, por sua vez, faria alusão a algo além da representação contida no dado, chegando ao limiar da cognição[9].

Em outras palavras, a informação pressupõe a depuração do conteúdo do dado.

Assim, o ordenamento pátrio preocupou-se em formalizar a proteção no que diz respeito ao elemento bruto, não lapidado, que determina cada indivíduo. Ou seja, o direito preocupa-se com à proteção aos dados pessoais, para que nem mesmo essa "pré-informação" esteja desprovida de garantias.

Adicionalmente, além da compreensão de dado, faz-se necessária delimitação do que seria um dado pessoal e um dado não pessoal, diferenciação esta que não se configura como meramente teórica. Os contornos dos conceitos de pessoal e não pessoal são de importância prática central para quase todas as atividades de processamento, pois o escopo de aplicação da Lei Geral de Proteção de Dados centra-se apenas no primeiro destes conceitos.

A título exemplificativo, não são entendidos como dados pessoais os dados de sensores climáticos sem ligação com pessoas. Isso porque não se conecta de maneira alguma a um indivíduo.

Assim, o cerne da diferenciação refere-se à verificação se os dados pessoais são dados que, direta ou indiretamente, se relacionam com uma pessoa singular identificada ou identificável. Todavia, a classificação de dados pessoais é dinâmica e, dependendo do contexto no qual o dado é inserido, ele pode ser ora considerado pessoal, ora não.

Em termos mais objetivos, o artigo 4º da Regulamento Geral de Proteção de Dados da União Europeia define dados pessoais como sendo qualquer informação relativa a uma

[9] Doneda, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020. p. 183.

pessoa singular identificada ou identificável (titular dos dados)[10]. Essa é também a linha seguida pela legislação brasileira, a qual delimita dados pessoais como uma informação relacionada a pessoa natural identificada ou identificável[11].

Nesse contexto, resta evidenciado que os dados pessoais são alusivos a um componente intrínseco e determinante para a constituição da própria personalidade de cada indivíduo. Em reconhecimento a isso, a sua proteção é considerada pelo direito brasileiro como um direito fundamental.

Todavia, tal status constitucional à proteção de dados é extremamente recente e teve seu início marcado por uma decisão paradigmática da Corte Superior Federal, mais especificamente no julgamento da ADI n. 6393, no qual discutia-se a constitucionalidade da Medida Provisória (MP) n. 954/20, que permitia o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP) com o IBGE, no intuito de auxiliar a produção estatística oficial durante a pandemia do COVID-19.

A Ministra relatora, Rosa Weber, destacou a ausência, na referida MP, de mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, conforme trecho abaixo:

> Enfatizo: ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando o caso, o anonimato dos dados compartilhados, a MP n. 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros. Essas considerações são corroboradas pela manifestação trazida aos autos pela Agência Nacional de Telecomunicações – ANATEL, que destacou necessária "a observância de extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações". E recomendou a adoção de medidas visando a adequar a medida à garantia dos princípios estabelecidos na Constituição Federal, na Lei Geral das Telecomunicações e na Lei Geral de Proteção de Dados, de modo a assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações.[12]

Essa decisão foi extremamente significativa para que houvesse uma mudança de chave na compreensão do que representa a proteção de dados, para a constituição da personalidade dos indivíduos. Mais emblemático ainda, especialmente porque confronta

---

[10] Em versão original, o conteúdo do artigo 4º da GDPR preconiza o seguinte: *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.

[11] LGPD, Art. 5º. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

[12] STF, Ação Direta de Inconstitucionalidade 6.387/DF, Rel: Min. Rosa Weber, publ. 07/05/2020.

a fundamentalidade do direito à proteção de dados com o princípio da supremacia do interesse coletivo, fazendo-o prevalecer no caso em específico.

À época do referido julgado, tramitava no Senado Federal o Projeto de Emenda à Constituição n. 17/2019[13], que buscava inserir na Carta Magna o direito à proteção de dados, especificamente dentro do rol do artigo 5º, de garantias fundamentais.

A emenda foi aprovada somente em 10 de fevereiro de 2022, de modo a constar a seguinte redação na Constituição Federal:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.[14]

A inclusão desta emenda constitucional traz consigo um manto protetivo muito maior, pois possibilita que a proteção de dados seja tratada em toda a sua fundamentalidade, bem como possibilita aos juristas fazerem um sopesamento desse direito com maior força entre os demais institutos jurídicos.

1.3. Dados sensíveis

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) define o conceito de dados sensíveis em seu artigo 5º, inciso II, nos seguintes termos:

> Art. 5º Para os fins desta Lei, considera-se:
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Trata-se de dados referentes a características íntimas cujo tratamento informatizado pode acarretar a discriminação do cidadão, seja pela etnia, raça, religião, orientação política, entre outros. Portanto, em caso de vazamento dos dados sensíveis, é alto o risco de que as pessoas venham a ser classificadas de forma preconceituosa, interferindo diretamente em seus direitos e liberdades individuais.

---

[13] UNIÃO FEDERAL. Câmara dos Deputados. Projeto de Emenda à Constituição n. 17/2019. Iniciativa do Senador Eduardo Gomes.

[14] BRASIL. Constituição da República Federativa do Brasil. Disponível em: https://www.google.com/search?q=cf&oq=cf&aqs=chrome.0.69i59j0i131i433i512j0i512j0i131i433i512j46i131i199i433i465i512j0i131i433i512j0i433i512j0i131i433i512l2j0i512.813j0j7&sourceid=chrome&ie=UTF-8. Acesso em: 24/04/2022.

No entanto, assim como a definição de dado pessoal não é estática, é igualmente possível que, por meio da utilização de algoritmos e inteligência artificial, obtenha-se um dado pessoal sensível a partir do dado pessoal não sensível.

Por isso, Laura Schertel fala em um "*tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias*"[15], concepção esta que se encontra em plena consonância com o princípio da não discriminação, elencado no art. 6º, inciso IX da LGPD[16].

1.4. Importância dos dados pessoais no mundo globalizado

Uma vez delimitados os conceitos basilares à plena compreensão desta pesquisa, é importante contextualizá-los na realidade prática.

A geração vigente desenvolve-se numa conjuntura de intensa troca informativa e absorção de novas tecnologias nas atividades diárias. Há quem entenda, até mesmo, pela ocorrência da "digitalização da sociedade"[17], conceito que remonta à comumente transposição da vida prática para o meio tecnológico, que se dá através do fluxo informativo das redes sociais, por exemplo, via fotos, vídeos e textos…

A sociedade chegou a um patamar no qual vigora a chamada economia informacional, em cujo contexto pode-se dizer que os dados despontam como um dos bens mais valiosos para a conjuntura atual. Obter o conhecimento acerca do funcionamento do mercado, tanto sob a perspectiva das tendências dos consumidores, como dos competidores, é uma das formas mais eficientes de se alcançar a fórmula para o sucesso.

Algumas empresas, inclusive, oferecem serviços "gratuitamente", quando na verdade os usuários pagam em forma de dados pessoais. Isso comprova o fato de que os dados são, verdadeiramente, uma riqueza.

Conforme já mencionado, é exatamente com o recrudescimento dos meios digitais, o qual consequentemente leva à circulação massiva de dados, que os debates sobre privacidade e sobre proteção de dados se tornaram tão importantes.

---

[15] MENDES, Laura Schertel. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Diss. Dissertação (Mestrado em Direito) –Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 63-64. Disponível em <http://repositorio.unb.br/handle/10482/4782>, 2008.

[16] LGPD, art. 6º, IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

[17] PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária *accountability*. RIL Brasília a. 57 n. 225. jan./mar. 2020.

Sendo assim, o que se observa é a grande massa de dados que passou a ser produzida e disponibilizada em ambientes de rede, fato que acaba por incentivar o contínuo surgimento de novas tecnologias que utilizam e fazem o tratamento de dados em grandes blocos informacionais.

Uma dessas inovações tecnológicas refere-se à chamada inteligência artificial. Consoante elucida Henrique Alves Pinto, diversos elementos incentivaram o uso cada vez mais habitual, como "*a habilidade de aprendizado pelas máquinas (...) além do avanço dos computadores, com a redução de seus custos e a criação de novas modalidades de algoritmos voltados à compreensão e à simulação da capacidade humana de cognição*"[18].

De maneira sintética e didática, podemos entender a inteligência artificial como uma tecnologia que simula justamente a inteligência humana, a fim de cumprir tarefas como o ser humano cumpriria. Para tanto, se vale dos algoritmos.

É o algoritmo que efetivamente faz toda a inteligência artificial funcionar, o qual pode ser entendido como sequências de instruções (regras matemáticas) e cálculos que são executados por um computador em uma ordem específica. Quanto mais dados ele tiver, mais preciso ele ficará.

Veja-se, o ser humano provavelmente não consegue recordar exatamente cada passo que deu durante a semana ou o mês. Contudo, o *smartphone* certamente tem todas as informações de localização pelas quais o seu usuário passou.

Tal fato evidencia o poder que as máquinas e equipamentos eletrônicos possuem no que tange ao monitoramento da vida dos cidadãos, bem como no armazenamento e processamento de dados e atividades de cada um.

Eventual programa ou sistema que tenha acesso a tais informações, sem respeitar princípios básicos de proteção à privacidade, poderia ocasionar prejuízos imensuráveis aos direitos de personalidade dos indivíduos. É precisamente isso que ocorreu no caso do sistema Pegasus, o qual será abordado no próximo capítulo, demonstrando-se uma ferramenta utilizada por entes de segurança estatais, cuja atuação é extremamente evasiva e desponta como um alerta aos limites do Estado frente aos direitos individuais.

[18] PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária *accountability*. RIL Brasília a. 57 n. 225. jan./mar. 2020. p. 45.

CAPÍTULO 2 – Utilização dos dados pelo Estado e o caso do Sistema Pegasus

2.1. O tratamento de dados na vigilância estatal

O fenômeno de automatização da máquina pública para gerir seus serviços e poder atuar com maior eficiência, indubitavelmente fez com que a proteção de dados dos indivíduos fosse dificultada. Isso é um processo natural, afinal, "*a proteção de dados pessoais começou a se estruturar com maior autonomia no momento em que o processamento automatizado de dados passou a representar, por si só, um fator de risco para o indivíduo"*[19].

Isto é, o próprio regramento de proteção de dados teve suas reflexões intensificadas em razão do aumento do fluxo informativo e tratamento massivo de dados. Normal, portanto, que as discussões e tensões entre esse regramento recrudesçam à medida que se intensifica a automação do Estado, o qual obtém um enorme repositório de dados acerca de seus cidadãos.

Ora, o ente público possui dados cadastrais e de identificação, detém os registros públicos, as informações de pagamento de salários e gestão de servidores públicos, os dados de declaração de imposto de renda, realiza o Censo - essencial para a definição de estratégias de políticas públicas e de decisões de investimentos -, realiza também pesquisas para monitorar e avaliar as condições de saúde e o desempenho do sistema de saúde brasileiro...

Esses são alguns exemplos de atividades que requerem do tratamento de dados para que sejam desempenhadas. Contudo, uma das mais delicadas e ensejadoras de debates refere-se à vigilância estatal.

Neste ponto, interessante retomar um caso emblemático para que seja feito um paralelo com a realidade brasileira.

O julgamento do caso *Katz v. United States*, de 1967, é um marco para o reconhecimento do direito à proteção de dados, pois representou a mudança no entendimento da Corte Norte-americana acerca da proteção à privacidade do indivíduo diante do poder de investigação do Estado.

---

[19] DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 22.

Trata-se de um caso no qual a polícia americana anexou um dispositivo eletrônico de escuta e gravação na parte externa da cabine telefônica, de modo que teria acesso irrestrito e sem consentimento às conversas dos indivíduos que ali se comunicassem.

A decisão judicial enquadrou a Quarta Emenda americana a este caso, com vistas a determinar a exigência de mandado judicial para o exercício da vigilância exercida por meios eletrônicos, além de ressaltar que os cidadãos devem ter sua expectativa de privacidade respeitada, para além de violações físicas à pessoa ou ao direito de propriedade[20].

A Corte entendeu que a referida Emenda constitucional rege não apenas a apreensão de itens tangíveis, mas também se estende ao registro de declarações orais, de sorte que o Estado deveria ter autorização para que pudesse interferir nesta esfera privada, intangível.

Trata-se de um precedente de suma relevância, pois demonstra que a vigilância estatal, por mais essencial que seja, deve respeitar os direitos invioláveis dos cidadãos. Veja que não é impossibilitado ao Estado praticar esse ato de vigilância, mas é preciso que haja o mandado judicial para tanto. A discricionariedade não pode ser absoluta!

Já na atualidade, as novas e mais desafiadoras dificuldades de conciliação da atuação de entes públicos com relação à necessidade de proteção ao direito à privacidade dizem respeito ao tratamento de dados massificados e a utilização de inteligência artificial (AI).

O aumento no uso de AI's por parte do Estado é uma tendência que vem se confirmando ao longo do tempo, sob o fundamento de cumprimento com o princípio da eficiência, inerente à atuação da Administração Púbica. As máquinas conseguem fazer um processamento de milhares de dados em poucos minutos com alta precisão, capacidade esta que o ser humano infelizmente não detém.

Assim, a utilização de inteligência artificial é muito importante, contudo, é preciso cuidado. Deve-se desmistificar a ideia de que ela é livre de experiências humanas, afinal, no momento da programação, quem definirá a sequência de algoritmos é um ser humano, podendo incorporar à sequência algorítmica as suas crenças e a sua formação cultural.

Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com determinada lógica, a qual é sempre utilitarista, isto é, cuida-se de um raciocínio que procura proporcionar a extração do máximo de proveito possível

[20] Riley v. California, 134 S. Ct. 2473, 2493, 2014. Disponível em http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

a partir de um conjunto de informações. Todavia, a maneira como essa lógica é pensada, organizada e programada, advém do ser humano.

Por conseguinte, a possibilidade de surgirem resultados discriminatórios não só é possível, como consideravelmente comum. Um exemplo bem manifesto disso é o caso do sistema de monitoramento e reconhecimento das delegacias do estado do Rio de Janeiro, cuja tecnologia teve como resultado a identificação de homens negros como o alvo mais recorrente[21].

Isso pode corresponder a uma seletividade voltada para determinados grupos sociais, ainda mais num país onde o racismo é tão intrínseco às relações sociais, como o Brasil.

Ocorre que, eventuais sistemas que perpetuem preconceitos e discriminações sociais não podem ser perpetuados pela Administração Pública, sob pena de violação ao princípio da dignidade da pessoa humana.

Nota-se, portanto, que a vigilância estatal configura como um polo de atração de tensões, haja vista que, no momento que o Estado vigia, ele necessariamente penetra, de alguma forma, na esfera de privacidade do indivíduo alvo. A grande questão a ser levada em consideração é a amaneira como ele faz isso e quais são os limites.

2.2. Novas tecnologias de vigilância adotadas por Estados: O que é o sistema Pegasus?

Denomina-se "sistema Pegasus" o *malware*[22] desenvolvido pela empresa de tecnologia Israelense chamada NSO, o qual é capaz de acessar qualquer celular (seja de sistema Android ou de IOS[23]) de modo a vigiar toda a sua atividade, ver todo o conteúdo

[21] Segundo o relatório da Defensoria Pública do Estado do Rio de Janeiro, realizado em 11 de setembro de 2020, "quanto a cor da pele, apenas dez são brancos(as), o que corresponde a 20%, considerando apenas os casos com informação. A informação sobre a cor da pele foi retirada dos registros policiais, o que provavelmente explica o uso de negra, ao invés de preta, uma vez que para o IBGE as pessoas de cor negra correspondem às negras e pardas". Disponível em: https://sistemas.rj.def.br/publico/sarova.ashx/Portal/sarova/imagem-dpge/public/arquivos/Relat%C3%B3rio__DPE-RJ.pdf. Acesso em 24.04.2022.

[22] Dentro do universo dos *softwares*, existem algumas classificações. Uma delas refere-se aos *malwares*, alusivos a qualquer tipo de *software* malicioso, desenvolvido para adentrar em dispositivos com a intenção de causar danos, seja infectando o sistema, seja explorando o dispositivo ou coletando informações de forma indevida. Os mais comuns são aqueles desenvolvidos para coletar alguns dados específicos, como senhas pessoais, elementos financeiros e registros médicos. Já o *spyware* é um conceito alusivo àqueles *malwares* que infectam dispositivos eletrônicos diversos com a intenção específica de registrar informações e rastreia a atividade dos aparelhos. No que tange ao sistema Pegasus, este pode ser entendido tanto como um *malware* ou, de modo mais específico, como um *spyware*.

[23] IOS é a sigla para "*iPhone operating system*", isto é, refere-se ao sistema operacional móvel da empresa Apple Inc.

do aparelho celular, ter acesso a e-mails e mensagens - inclusive, as mensagens criptografadas do *WhatsApp* ou de qualquer outro programa de conversa simultânea - e, até mesmo, permite que o invasor escute as ligações efetuadas pelo aparelho hackeado, e ligue a câmera ou o microfone, tudo isso sem que o usuário do telefone saiba.

Para ser espionado, o aparelho alvo apenas precisa estar conectado à internet e receber uma mensagem de texto ou uma ligação pelo *WhatsApp* e, imediatamente, ativar-se-á o programa sem que o usuário perceba a invasão.

Em outras palavras, o programa configura-se como uma espécie de espião de bolso, cujo vetor de disseminação é muito agressivo, afinal, quem tem seu celular infectado encontra-se numa situação na qual todos os dados disponíveis em seu aparelho pessoal são expostos, sem qualquer tipo de consentimento e sem sequer saber que está sendo vigiado.

O referido sistema foi desenvolvido pelo NSO *Group* com o intuito de ser comercializado especificamente para entes estatais. Inclusive, no site da companhia israelense, sua própria descrição deixa claro que o público-alvo de seus serviços são agências governamentais, cuja atuação seria especificamente para prevenir e investigar ameaças de terrorismo e crimes, tudo isso envolto no objetivo maior de "*salvar milhares de vidas ao redor do globo*"[24].

Em síntese, a ideia vendida por esta empresa de *cyber* inteligência é de que os criminosos e terroristas possuem acesso a inúmeras armas e ferramentas extremamente sofisticadas para programarem suas ações e atacarem os alvos que lhes convém e, em contrapartida, os Estados estariam sendo deixados para trás. Isso porque as nações e suas leis de acesso a dados acabam por burocratizar e dificultar a atuação da segurança estatal, limites legais estes que não se aplicam aos criminosos.

Pois bem. Neste ponto, é interessante abordar uma curiosidade: Israel figura como um país referência no quesito segurança e vigilância estatais. Isso porque as forças militares são culturalmente muito fortes naquele país[25], assim, muito do que temos de

---

[24] Em seu site, a NSO *Group* menciona seu nicho bem específico de clientes, qual seja entes governamentais, veja-se: "*Our products help licensed government intelligence and law-enforcement agencies lawfully address the most dangerous issues in today's world. NSO's technology has helped prevent terrorism, break up criminal operations, find missing persons, and assist search and rescue teams".* Disponível em: https://www.nsogroup.com/. Acesso em 09.04.2022.

[25] *Much of the Israeli arms industry is Government-owned, and exact financial data are secret. But according to widely-used estimates, as many as 140,000 Israelis - 10 percent of the work force - are involved in manufacturing or selling military hardware. "Israeli arms manufacturers have reached such a level of production and importance within the Israeli economy that exporting weapons has become an economic imperative," observed Aaron S. Klieman, a Tel Aviv University political scientist*. FRIEDMAN, Thomas L. How Israel's economy got hooked on selling arms abroad.

cyber segurança, principalmente governamental, vem de pesquisas militares realizadas lá. O próprio NSO teve início como uma *startup* criada por um ex-militar israelense, que utilizou de todo o seu conhecimento adquirido nos anos trabalhados e todas as influências cultivadas neste período.

Ocorre que, as empresas de *cyber* inteligência ali desenvolvidas acabam por criar sistemas que possivelmente extrapolam os limites de interferência à vida privada dos cidadãos e, inevitavelmente, desrespeitam as regulações de proteção de dados de outras nações.

Qual seria o limiar para a intervenção dos Estados em prol da defesa nacional e segurança pública? É o que abordaremos nos tópicos seguintes.

2.3. Utilização do sistema Pegasus

No caso específico do sistema Pegasus, ao que se sabe, o NSO ofereceu o seu produto para autoridades de diversos países, como a Rússia, o México, a China e a Alemanha, por exemplo. Quanto a este último, a informação que circula é de que o Departamento Federal de Investigações da Alemanha (BND) se interessou pelo *spyware*, em razão do inequívoco poder que esse programa dispõe. Contudo, a negociação não foi concretizada justamente por verificarem que a sua utilização confrontaria as leis de privacidade que lá vigoram.

De todo modo, a partir do momento que o sistema Pegasus tornou-se de conhecimento público, a empresa NSO *Group* alegou que seu *software* se destina ao uso contra criminosos e terroristas e está disponível apenas para militares, policiais e agências de inteligência de países com bom histórico de direitos humanos.

De fato, é difícil cravar um número exato de telefones que foram infectados pelo referido programa, assim como o radar de incidência de sua aplicação, mas, independentemente de a ferramenta ter sido comercializada apenas para entes de vigilância pública, não deixa de figurar como um instrumento que viola frontalmente os direitos à privacidade e à proteção de dados. Frisa-se, ainda, que a sua utilização por parte de Estados desponta como uma situação absolutamente preocupante, afinal, se sequer o

---

https://www.nytimes.com/1986/12/07/business/how-israel-s-economy-got-hooked-on-selling-arms-abroad.html. Acesso em: 19/04/2022.

Estado respeita as suas próprias leis de proteção de dados, imagine-se a insegurança jurídica que isso pode levar.

Algumas organizações uniram seus esforços para tentar entender melhor do que se tratava esse *software* e qual teria sido a extensão de sua utilização. Uma dessas iniciativas refere-se ao consórcio jornalístico coordenado pela *Forbbiden Stories*, denominado "*The Pegasus Project*"[26].

De acordo com este consórcio, os dados vazados mostraram que o Pegasus foi utilizado em 21 (vinte e um) países e, pelo menos 85 (oitenta e cinco) defensores dos direitos humanos e 180 (cento e oitenta) jornalistas foram selecionados como alvos em países como Índia, México, Hungria, Marrocos e França, entre outros. Os alvos potenciais também incluem acadêmicos, empresários, advogados, médicos, líderes sindicais, diplomatas, políticos e vários chefes de Estado.[27]

Assim, apesar das repetidas alegações do NSO *Group*, de que suas ferramentas são usadas exclusivamente para atacar criminosos e terroristas graves, a realidade prática aponta para situação diversa. O fato de tantos jornalistas, ativistas e, até mesmo, políticos estarem entre os alvos, demonstra que a finalidade deste sistema de vigilância vai para além de fins voltados para a segurança pública.

Dentre os possíveis alvos, figuram, por exemplo, o político, empresário, ativista e ex-líder sindical sul-africano Cyril Ramaphosa, o ex-primeiro-ministro do Paquistão, Imran Khan, o parlamentar indiano Rahul Gandhi, membro do Partido do Congresso Nacional Indiano, bem como o presidente da França, Emmanuel Macron. No que se refere a este último, não há confirmação de que ele tenha sido efetivamente espionado, porém, o porta-voz do governo francês, Gabriel Attal, disse que os protocolos de segurança do presidente estavam sendo adaptados à luz do incidente e, por isso, seus números de telefone foram trocados.

Veja-se que, nem mesmo importantes políticos estão protegidos das ferramentas de espionagem utilizadas por Estados. Além de interferir na esfera de direitos da personalidade dos referidos políticos, ao que tudo indica, o sistema Pegasus também foi utilizado com uma finalidade absolutamente distinta daquela a que se propõem, que seria a vigilância a criminosos.

---

[26] O trabalho colaborativo foi resultado da união de dezessete organizações jornalísticas em dez países, bem como utilizou-se de suporte técnico, realizado pelo Laboratório Técnico da Anistia Internacional.

[27] Informação disponível em: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/. Acesso em 09.04.2022.

Consoante se depreende das informações ora expostas, o poder de vigilância que este *software* possui é capaz de angariar informações que, se utilizada de maneira enviesada, podem violar a supremacia nacional das nações, interferir em campanhas eleitorais e manipular a condução de questões internacionais.

Este é um dos grandes problemas das ferramentas de vigilância digital, pois a capacidade de violação da intimidade dos indivíduos costuma ser muito alta, ao ponto de gerar efeitos irremediáveis e que atinjam âmbitos muita maiores que apenas o individual.

Além de tudo que já fora exposto, os dados vazados sobre o Pegasus sugerem que o *spyware* é usado de forma muito mais descuidada do que o anunciado. No relatório de transparência publicado em junho de 2021, o NSO *Group* enfatizou que o referido programa "*não era uma tecnologia de vigilância em massa*" e era "*usado apenas onde havia uma aplicação legítima da lei ou motivo de inteligência*"[28]. No entanto, mais de 10.000 (dez mil) números de telefone foram selecionados para vigilância apenas pelo ente estatal marroquino da empresa israelense, durante um período de dois anos.

Desta afirmação por parte do NSO, pode-se depreender um nítido desvio de finalidade, bem como de escopo e extensão de atuação do *mallware*, elementos que infringem frontalmente os princípios basilares da proteção de dados.

De mais a mais, interessante notar que, a utilização do Pegasus se deu em países que possuem leis especificamente voltadas à proteção de dados pessoais. O México, por exemplo, possui, desde 2010, a *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, cuja aprovação foi considerada um grande avanço para o direito das pessoas de controlar o tratamento de suas informações pessoais. Em contrapartida, a realidade mostra que os órgãos de vigilância do país utilizam-se de uma ferramenta que desrespeita a vida privada dos indivíduos de maneira completamente invasiva.

O ex-diretor da Agência de Inteligência Criminal Mexicana (AIC), Tomás Zerón, foi o responsável por fechar o contrato do sistema Pegasus e, fontes das agências de segurança mexicanas ouvidas pelo *The Pegasus Project*, declararam que Zerón fazia uso do sistema na AIC de maneira descontrolada. Ele ficou conhecido no país por ser o responsável por dois grandes casos: a recaptura do traficante Joaquín "El Chapo" Guzmán

[28] Disponível em; https://forbiddenstories.org/about-the-pegasus-project/. Acesso em: 09.04.2022.

e o desaparecimento dos 43 estudantes normalistas de Ayotzinapa[29]; contudo, inobstante tais capturas de criminosos, é necessário dar foco para o fato de que a espionagem de telefones celulares foi utilizada de maneira recorrente pelo representante mexicano. Imagine-se quantas pessoas tiveram sua privacidade violadas neste contexto.

Ao fim e ao cabo, depreende-se que a abrangência da utilização do sistema Pegasus foi consideravelmente acentuada, o que demonstra o quão frágeis são as proteções à intimidade dos indivíduos, especialmente na sociedade informativa.

É evidente a necessidade de algum tipo de limitação e penalização para tais atos.

Questionado, o *NSO Group* alegou que não pode ser imputado pelo uso dessa aplicação, porque quem usou a ferramenta são os governos e quem deve fazer seu manuseio em respeito às próprias regras de proteção de dados são eles próprios.

Pois bem. Certamente, os agentes e entidades de Estado devem ser imputados quanto às violações praticadas, até mesmo como uma forma de evidenciar que a atividade do setor público também deve ser fiscalizada e responsabilizada.

No entanto, isso não tira o fato de que os criadores do *malware* produziram uma ferramenta sabendo do imensurável poder de violação à privacidade que ele possui. A sistemática geral de proteção de dados já é bem difundida, de modo que certamente a empresa já tinha conhecimento que o sistema Pegasus a infringe, desrespeitando os princípios da necessidade, da finalidade e do livre acesso, por exemplo. Nesse sentido, não há como eximir-se de sua responsabilidade em comercializar tal ferramenta.

De todo modo, a presente pesquisa pretende averiguar as limitações impostas pelo direito à privacidade e à proteção de dados sob a ótica do Estado, motivo pelo qual será abordado no próximo capítulo o âmbito de incidência legal de aplicação desses direitos, bem como as tensões principiológicas que o poder público tem de encarar.

[29] GUERRA, Dolores. Pegasus e a Ciber Espionagem Israelense no México. Memo: 2021. Disponível em: https://www.monitordooriente.com/wp-content/uploads/2021/08/PEGASUS-E-A-CIBER-ESPIONAGEM-ISRAELENSE-NO-MEXICO-final-.pdf. Acesso em 09.04.2022. p. 04.

CAPÍTULO 3 – Intersecção entre a vigilância e privacidade

3.1. Âmbito de incidência, bases legais para a atuação estatal

No que tange à atuação do Estado quanto ao tratamento de dados, naturalmente a sistemática normativa deve ter nuances distintas das aplicáveis à atividade dos entes privados.

Válido que se faça uma breve retomada a uma das primeiras leis especificamente sobre a regulação da atuação do poder público no que diz respeito aos dados pessoais, o chamado *Privacy act*, de 1974. Este diploma legislativo determina que as agências divulguem seus sistemas de registros por meio de publicação no Registro Federal, fornece aos indivíduos um meio para buscar acesso e alteração de seus registros, bem como proíbe a divulgação de registros sobre um indivíduo sem o seu consentimento, a menos que a divulgação esteja de acordo com alguma das exceções legais.

Verifica-se que essas são atribuições muito características da atividade pública, porque se relacionam com os princípios administrativos da publicidade e da transparência, assim como se preocupam com registros especificamente comuns de serem mantidos pelo Estado.

No entanto, para uma análise mais apurada em relação à atividade específica de vigilância estatal, é interessante mencionar seus âmbitos de incidência próprios.

O primeiro deles diz respeito às atividades de identificação criminal por parte do poder Público, que se enquadram como medidas de segurança pública e de investigação e repressão de infrações penais. Dentro dessa atividade, é possível citar (i) o tratamento de dados colhidos pela utilização de tornozeleiras eletrônicas, (ii) a atuação da polícia judiciária para investigação de atividades criminosas, objetivando instruir inquéritos policiais e processos penais, (iii) a coleta e análise de imagens obtidas por *drones* ou pela instalação de câmeras de monitoramento em ambientes públicos, assim como (iv) a análise dos sistemas de reconhecimento facial que podem estar acoplados às referidas câmeras de vigilância[30].

Relativamente a este último mecanismo, observa-se que os dados coletados pelos sistemas de vigilância públicos acabam por atribuir elementos identificadores aos

[30] O artigo de Jaqueline Abreu citas esses e demais exemplos de atividades de tratamento de dados para fins de vigilância estatal. ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós– LGPD. In: BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 282 – 299.

indivíduos monitorados pelas câmeras, de modo que a pessoa natural identificável passa a ser identificada pelo sistema de reconhecimento facial.

Ainda neste ponto, frisa-se que as operações de tratamento de dados para a execução da vigilância estatal também podem partir do aproveitamento de dados que originalmente foram coletados por órgãos estatais, com intuito alheio à segurança pública. Como a utilização de documentação civil, registro escolar, registro de condutores, entre outros. Para tanto, é necessária a denominada interoperabilidade entre os sistemas, conceito este que abordarmos mais à frente.

Da mesma forma, o poder público pode se utilizar de dados que foram obtidos por entes privados, tal qual em casos de reutilização de câmeras privadas e aproveitamento de controle biométrico ou reconhecimento facial para acesso a empresas privadas.

Diante de todos esses exemplos, como o poder estatal tem deveres de realização de políticas públicas e manutenção da segurança nas sociedades e do bem-estar coletivo, observa-se que é preciso que a coleta e o tratamento de dados tenham algumas adaptações para a dinâmica estatal.

Logo, a operabilidade de dados por parte do Estado deve obedecer a normas específicas, as quais almejam estruturar premissas básicas para um adequado tratamento de dados, bem como para possibilitar ao seu titular ter ciência da qualidade tanto do banco de dados, quanto do tratamento.

Nada obstante, antes de adentrar na análise das bases legais em si, interessante apontar que a disciplina de proteção de dados, em razão de possuir um âmbito de incidência muito amplo nas relações civis, está elencada em diversos diplomas normativos.

Além da Lei Geral de Proteção de Dados, o Código Civil, o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei das Telecomunicações e a Lei do Cadastro Positivo, por exemplo, também abordam a questão da proteção à privacidade, sem contar a Constituição Federal, que se posiciona como o guia para uma interpretação coesa do ordenamento.

A fim de viabilizar uma aplicação coerente entre os aparentes conflitos legislativos, a teoria do diálogo das fontes[31], de Cláudia Lima Marques, desponta como a

[31] Afirma Cláudia Lima Marques que "*Aceite-se ou não as razões a pós-modernidade, a verdade é que, na sociedade complexa atual, com a descodificação, a tópica e a microrrecodificação (como a do CDC) trazendo uma forte pluralidade de leis ou fontes, a doutrina atualizada está à procura de uma harmonia ou coordenação entre estas diversas normas do ordenamento jurídico (concebido como sistema). É a denominada "coerência derivada ou restaurada" ("cohérencedérivée ou restaurée"), que procura uma*

chave para a aplicação adequada do direito à proteção de dados. Segundo essa lógica, os operadores do direito não utilizam uma norma em exclusão a outra, mas buscam uma alternativa de coordenação dos diferentes diplomas normativos para o mesmo caso em concreto.

Uma vez delineada essa questão de intersecção legislativa, parte-se para a análise do escopo normativo aplicável ao Estado.

Como se sabe, a LGPD, foi inspirada no Regulamento Geral Europeu para a Proteção de Dados – GDPR (Regulamento UE 2016/679), principalmente no que tange à característica de Lei geral, acobertada por um conteúdo de teor bastante próximo ao principiológico.

Neste sentido, explicam Bruno Bioni e Laura Schertel:

> Apesar das diferentes técnicas legislativas, há uma convergência perceptível entre os princípios previstos no RGPD e na LGPD. Essa convergência pode ser atribuída menos a uma influência direta do processo legislativo europeu na lei brasileira do que a um longo processo de construção de um consenso transnacional acerca dos princípios básicos que regem essa matéria.[32]

Assim, como a opção do legislador foi por adotar o modelo de proteção de dados de caráter principiológico, muitas das normas são abstratas e requerem um sopesamento entre si, dentro da análise específica do caso prático.

Porém, é comum que haja a dúvida acerca da aplicação dos princípios elencados na LGPD para casos enquadrados no seu artigo 4º, cuja redação expõe que "*esta Lei não se aplica ao tratamento de dados pessoais: (...) 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*"[33].

Ou seja, como a vigilância estatal está vinculada a todas essas hipóteses, a Lei Geral de Proteção de Dados não é tomada como o diploma legislativo de referência para

---

eficiência não só hierárquica, mas funcional do sistema plural e complexo de nosso direito contemporâneo. (...) *Há mais convivência de leis com campos de aplicação diferentes, do que exclusão e clareza. Seus campos de aplicação, por vezes, são convergentes e, em geral diferentes, mas convivem e coexistem em um mesmo sistema jurídico que deve ser ressistematizado. O desafio é este, aplicar as fontes em diálogo de forma justa, em um sistema de direito privado plural, fluido, mutável e complexo*. MARQUES, Cláudia Lima. Superação das antinomias pelo Diálogo das Fontes: O modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. Revista da Escola Superior da Magistratura de Sergipe (ESMESE), nº 7, 2004, p. 29.

[32] MENDES, Laura Schertel; BIONI, Bruno. O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor. Vol. 124. Ano 28. p. 157-180. São Paulo: Editora RT, jul-ago 2019. p. 165.

[33] BRASIL. **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: 02/02/2022.

regulação e orientação da atuação do Estado, especificamente no que diz respeito ao âmbito de vigilância. Isso evidencia, portanto, a urgência de uma legislação específica para o tema.

Contudo, de todo modo, no que concerne aos princípios da LGPD, por uma análise dialógica de fontes normativas, extrai-se a conclusão de que toda a sua parte principiológica é sim aplicável às atividades de vigilância estatal, bem como a qualquer norma que direta ou indiretamente estabeleça relação com o tema da proteção de dados.

Isso porque, o Decreto n. 10.046/2019[34], que dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública Federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, possui como um de seus fundamentos o Capítulo IV da Lei n. 13.709, de 14 de agosto de 2018 (LGPD)[35].

Assim, considerando (i) a hierarquia das normas, de sorte que a norma geral deve se sobrepor à específica e (ii) o fato de que o mencionado capítulo IV da LGPD versa sobre o tratamento de dados pessoais pelo poder público, sobre o qual recaem todos os princípios da referida lei - conforme preconiza o artigo 26 da Lei Geral[36] -, temos que, deve haver a adequação e o respeito aos termos da LGPD para que o mencionado Decreto tenha a sua aplicação legítima.

De forma sintética, as disposições acerca da governança no compartilhamento de dados no âmbito da Administração Pública Federal – objeto do Decreto n. 10.046/2019 – só serão legítimas se houver o respeito aos fundamentos da Lei Geral n. 13.709/2018, incluindo suas disposições principiológicas.

Neste sentido, os princípios são aplicáveis ao tratamento de dados pelo Estado, até mesmo no que tange à vigilância estatal.

O diferencial está em algumas exceções elencadas na LGPD. Uma delas refere-se aos dados sensíveis, que foram conceituados no tópico 1.3 deste presente trabalho. É certo que, para a execução de algumas políticas públicas, como o planejamento estratégico de ações de saúde e de segurança pública, o manuseio de dados sensíveis é essencial.

Assim, para o poder público, os dados sensíveis podem ser usados sem o fornecimento de consentimento do titular, nas hipóteses em que for indispensável para o

---

[34] O Decreto n. 10.046/2019 possui como fundamentos: "o disposto no art. 5º, caput, inciso XXXIII, no art. 37, § 3º, inciso II, e no art. 216, § 2º, da Constituição, na Lei nº 12.527, de 18 de novembro de 2011, no art. 11 da Lei nº 13.444, de 11 de maio de 2017, e no Capítulo IV da Lei nº 13.709, de 14 de agosto de 2018".

[35] O Capítulo IV - Do tratamento de dados pessoais pelo poder público.

[36] LGPD, Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.[37]

Ocorre que, para que haja essa facilitação para os órgãos e pelas entidades públicas, o artigo 11, § 2º [38] institui o dever de dar publicidade à referida dispensa de consentimento.

De todo modo, o consentimento ainda é uma questão nebulosa dentro da conjectura de tratamento de dados por entes públicos. Conforme bem aponta Miriam Wimmer, "*sob uma perspectiva pragmática, a possibilidade de revogação do consentimento a qualquer tempo representa outro grande inconveniente para seu uso como base legal para o tratamento de dados pessoais pelo Poder Público*"[39].

Outro elemento característico do tratamento de dados pelo poder público é interoperabilidade, caracterizada como a capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados[40].

A necessidade de uma organização para comunicação entre sistemas é de suma relevância para que o Estado tenha os meios necessários à execução de suas políticas públicas, por isso a legislação prevê a interoperabilidade. Contudo, ela deve observar a legislação e as recomendações técnicas estabelecidas pelo Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp do Poder Executivo federal, e, ainda, as recomendações do Comitê Central de Governança de Dados.

Notadamente, é basilar que haja organizações estatais que regulem e atuem diretamente na organização desses sistemas, para que o princípio da proteção de dados referente à finalidade não seja violado.

Outrossim, o Decreto 10.046/2019 elenca em suas diretrizes que os mecanismos de compartilhamento e interoperabilidade também devem obedecer ao princípio da

---

[37] Segundo o art. 11, da LGPD: O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

[38] LGPD, Art. 11, § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

[39] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 286. p. 292.

[40] Conceito extraído do Art. 2º, XVIII do Decreto 10.046/2019.

necessidade, isto é, sua realização deve se limitar às necessidades de negócio dos órgãos e entidades públicas operadoras dos dados [41].

Outros elementos de proteção à privacidade são elencados neste decreto, determinando-se que os dados pessoais deverão ser tratados respeitando-se o direito à preservação da intimidade e à privacidade da pessoa natural, à proteção dos dados, bem como às normas e aos procedimentos previstos na legislação.

Tudo isso evidencia uma propensão dos comandos normativos de se complementarem e reforçarem, situação extremamente benéfica para a harmonia da sistemática de proteção aos direitos da personalidade.

Por fim, conforme já mencionado anteriormente, tanto o direito à privacidade, quanto à proteção de dados configuram-se como normas de caráter constitucional, previstos entre o rol de direitos fundamentais, no artigo 5º, incisos X e LXXIX, respectivamente.

Logo, o Estado tem de moldar a sua atuação de maneira que não comporte violações aos mencionados direitos da personalidade. É preciso, por exemplo, compreender quais são os limites do que é necessário de ser tratado, para que se atinja os fins pretendidos pelo ente estatal no momento da coleta de informações dos cidadãos.

De igual maneira, deve ser disponibilizado um canal para que cada indivíduo possa ter acesso às informações que o Estado guarda sobre si, afinal, eventual elemento errôneo poderá gerar prejuízos na vida civil daquele titular.

Possibilitar o acesso por parte do titular, bem como organizar meios para que ele possa notificar algum eventual erro também se configuram prerrogativas inerentes ao direito de personalidade e autodeterminação.

Vale fazer um adendo, no sentido de demonstrar que a presente pesquisa considera a dificuldade de conciliação entre a atuação do Estado - que deve seguir os princípios, por exemplo, da publicidade e da supremacia do interesse público -, com a proteção à vida privada e à intimidade de seus cidadãos. Apesar disso, se trata de uma atividade que obrigatoriamente deve ser feita pelo poder público, e, portanto, deve ser discutida também pela academia e pelos operadores do direito.

3.2. O sistema Pegasus sob um olhar principiológico da proteção de dados

[41] Art. 3, inciso III do Decreto 10.046/2019.

Com o intuito de tangenciar os princípios da proteção de dados, de modo a constatar o quão invasivo podem ser os sistemas de vigilância estatal, remonta-se aos princípios vigentes no ordenamento brasileiro, cuja inspiração vem do Regulamento Geral de Proteção de Dados da União Europeia.

Trazendo o caso do sistema Pegasus para a realidade brasileira, conclui-se que seu uso acaba por confrontar absolutamente todos os princípios explícitos da Lei Geral de Proteção de Dados[42], os quais são aplicáveis também a atividades de vigilância estatal, consoante já mencionado.

Passa-se, portanto, a demonstrar o mencionado desrespeito aos princípios da LGPD.

De acordo com a ordem elencada na própria Lei Geral, os primeiros princípios referem-se ao da finalidade e ao da adequação, os quais pressupõem, respectivamente, que o tratamento de dados deve (i) ser realizado para propósitos legítimos, específicos e explícitos, que precisam ser estritamente informados ao titular, bem como deve (ii) ser compatibilizado às referidas finalidades repassadas ao titular dos dados.

Ora, como se sabe, o sistema Pegasus é ativado sem que o titular dos dados saiba da invasão ao seu celular. Assim, não existe sequer um parâmetro de finalidade e nem mesmo de adequação para aplicação desses princípios.

Outrossim, mesmo se for considerada a finalidade implícita de vigilância estatal - o que em si já seria problemático, pois uma finalidade de tratamento de dados deve ser bem definida, não podendo ser algo tão abrangente, sem limitações -, é facilmente

[42] Os princípios da LGPD estão elencados em seu artigo 6º, conforme vejamos: 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.

verificável que a prática de utilização do sistema foi além do monitoramento a possíveis terroristas ou criminosos.

Conforme mencionado no tópico anterior, muitos dos alvos do *mallware* tiveram um cunho essencialmente político, afinal, a enorme gama de jornalistas, ativistas, líderes sindicais, diplomatas e políticos que figura na lista de prováveis invadidos demonstra uma tentativa de governos monitorarem o que a mídia e os agentes ativos na promoção de projetos sociais estão organizando, ou quais informações eles têm acesso.

Em seguida, a Lei n. 13.709/2018 delineia o princípio da necessidade, o qual refere-se como a "*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*".

Tal comando principiológico conjectura que as informações de identificação pessoal devem ser mantidas em mínimo necessário pelo operador dos dados, de modo que qualquer lugar possível de identificabilidade e vinculação de informações pessoais devem ser minimizadas em consonância com o que é necessário para os fins especificados.

Aplicando ao caso em análise, sequer se sabe quais dados foram mantidos em armazenamento, de modo que os entes estatais – que utilizaram o sistema Pegasus sob a justificativa de vigilância estatal – conseguem obter absolutamente todos os dados do aparelho celular de seus alvos. Isso certamente não se refere a uma coleta do mínimo necessário para o tratamento de dados, opondo-se frontalmente ao princípio da necessidade.

Seguindo o rol principiológico da LGPD, há os princípios da transparência e do livre acesso, que exigem ao operador de dados dar aos titulares informações claras e precisas sobre o seu tratamento, tanto em relação a quem terá acesso, quanto ao que se pretende com o referido tratamento. Ademais, é preciso que haja a garantia de consulta facilitada à integralidade de seus dados pessoais, bem como sobre a forma e a duração do tratamento.

Vincula-se a este ponto, outro princípio da Lei Geral, qual seja o da qualidade. Segundo tal preceito, é preciso que haja a garantia ao titular dos dados de que as suas informações mantidas pelo operador são verdadeiras e que estão atualizadas, bem como devem estar alinhadas com o propósito do tratamento.

O respeito a esses princípios é essencial para estabelecer responsabilidade e confiança entre o titular e o operador dos dados. Assim, as informações sobre as políticas

e práticas relacionadas ao gerenciamento de informações pessoais devem ser prontamente disponibilizadas para os indivíduos.

Por óbvio, os titulares dos dados obtidos pelo sistema Pegasus não possuíam livre acesso para consultá-los, nem mesmo para verificar sua qualidade, muito menos tinham informações acerca da realização do tratamento, afinal, sequer sabiam que estavam sendo vigiados.

Seguindo, a LGPD concebe os princípios da segurança e da prevenção, que se referem à utilização de medidas técnicas e administrativas que garantam o seguro tratamento de dados, evitando possíveis invasões, perdas, tratamentos inequívocos, utilização de dados em situações que violem a dignidade do seu titular, assim como, devem ser adotados métodos para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Sobre tais princípios, a análise inicia-se pela constatação de que, no caso do sistema Pegasus, a própria obtenção dos dados figura-se como uma invasão completamente inesperada. Assim, qualquer tratamento que venha após, configura-se como uma lesão ao direito à privacidade.

Outro princípio elencado é o da não discriminação, o qual está em ampla consonância com artigo 2º, inciso VII da LGPD, segundo o qual são fundamentos do tratamento de dados pessoais *os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais*.

Assim, a vedação a tratamentos cujo fim seja discriminatório, abusivo ou ilícito é uma proteção à própria dignidade da pessoa humana. Tal garantia é de suma relevância, pois os indivíduos encontram-se em posição vulnerável quanto ao uso de seus dados perante o Estado, especialmente com o considerável avanço de tecnologias de processamento de dados em escala massiva por organismos públicos.

No que tange à vigilância estatal, o potencial de discriminar e classificar os indivíduos é ainda mais latente, pois o Estado se propõe a vigiar e captar informações sobre os indivíduos sob a justificativa de manter a segurança pública. Assim, a esfera privada é interferida em prol do bem coletivo.

De todo modo, não se sabe quais eram os critérios para a invasão de aparelhos eletrônicos pelo Pegasus, nem a maneira como o seu tratamento era efetuado, o que em si já se configura como um risco ao princípio da não discriminação. Chama a atenção também o fato de que tantos jornalistas e ativistas sociais foram alvo do *mallware*.

Por fim, figuram-se os princípios da responsabilização e prestação de contas, que correspondem ao dever do agente em demonstrar a 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.

Entretanto, não houve responsabilização frente ao caso. Viu-se uma pressão à Israel, diante da latente necessidade de haver algum tipo de regulação para as inúmeras empresas de *cyber* segurança que lá surgem. Contudo, em termos de responsabilização dos agentes, de fato não houve, bem como ainda se sabe pouco do caso, restando descaracterizada qualquer possibilidade de configuração da prestação de contas.

3.3. Equilíbrio entre os princípios da Administração Pública e os direitos à privacidade e à proteção de dados

A delicada relação entre vigilância e privacidade deve ser analisada sob a ótica dos princípios constitucionalmente estabelecidos tanto no viés de atuação estatal, como no âmbito dos direitos individuais; contudo, essa conciliação é bastante complexa.

A economia informacional e a intensa troca de dados fizeram com que a esfera da privacidade ficasse cada vez mais vulnerável. Como nota Lyon, podemos inclusive falar no termo "Sociedade da Vigilância", que muito bem se aplica à realidade atual:

> A ascensão da "Sociedade da Vigilância" se conecta, portanto, de maneira inextricável, com o crescimento do moderno Estado-nação. À medida que se ampliava o escopo das tarefas administrativas necessárias, a organização burocrática evoluía como mecanismo de coordenação de atividades. As vidas diárias das pessoas tornaram-se, assim, crescentemente sujeitas à documentação, dentro dos arquivos abrangentes do Estado burocrático. Tudo isso pode ser encarado a partir de duas perspectivas: como uma tentativa de impor novas formas de ordem, de controlar situações que ameaçavam ruir no caos com a formação do agora familiar mundo urbano-industrial, e como o resultado da busca por plena cidadania e participação democrática na nova ordem, que requeria, para o tratamento equitativo, que os indivíduos fossem identificados, registrados e documentados em dossiês que se multiplicavam.[43]

Com a polêmica do caso Pegasus, essa sensação de que "*as vidas diárias das pessoas tornaram-se crescentemente sujeitas à documentação*" ficou perfeitamente evidente. Uma jornalista do Azerbaijão Khadija Ismayilova, que fora alvo do *spyware*, declarou para *The Forbidden Stories* que todos aqueles indivíduos que também foram

[43] LYON, D. The electronic eye. The rise of surveillance society. Minneapolis: University of Minnesota Press, 1994. P. 33.

invadidos compartilharam uma sensação geral de impotência quando souberam do ataque cibernético sofrido. Segundo suas próprias palavras, "*temos recomendado uns aos outros esta ferramenta ou aquela ferramenta, como manter [nossos telefones] cada vez mais protegidos dos olhos do governo*", e continua afirmando que "*eu percebi que não tem jeito. A menos que você se tranque em uma tenda de ferro, não há como eles não interferirem em suas comunicações.*"[44]

O nível de invasão ocasionado por esse sistema é absolutamente insustentável dentro de um ordenamento que reconheça a existência de direitos da personalidade.

Todavia, por mais que seja latente a necessidade de observância a esses direitos, quando o debate é em relação ao tratamento de dados por parte da Administração Pública, não se pode olvidar que ela deve atender aos princípios explícitos, dispostos no artigo 37 da Constituição Federal[45], como o da publicidade e o da eficiência, mas também se requer respeito aos princípios intrínsecos, como o da supremacia do interesse público sobre o privado e o da transparência.

Os 4 (quatro) princípios mencionados são os que comumente estão mais associados ao direito à privacidade, os quais passa-se a tratar.

Primeiramente, o princípio da eficiência pode ser definido como "*o que se impõe a todo agente público de realizar suas atribuições com presteza, perfeição e rendimento funcional, (...) exigindo resultados positivos para o serviço público e satisfatório atendimento das necessidades da comunidade e de seus membros*" [46], consoante leciona Hely Lopes.

Este preceito está intimamente ligado com o recrudescimento da utilização de máquinas de processamento de dados no âmbito estatal. É evidente que a inteligência artificial, bem como os mecanismos digitais para armazenamento e processamento de dados trazem maior eficiência para a realização da atividade Pública, pois sua capacidade de atuação é infinitas vezes mais célere que a de um ser humano, especialmente para análise de dados em massa.

Nessa toada, embora o processamento e o compartilhamento de dados sejam funções inevitáveis na sociedade atual, é essencial que o órgão que realiza o processamento cumpra a lei.

---

[44] Declaração retirada de: https://forbiddenstories.org/about-the-pegasus-project/. Acesso em 22.04.2022.
[45] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência (...).
[46] MEIRELLES, Hely Lopes. Direito administrativo brasileiro. São Paulo: Malheiros, 2003. P. 102.

A utilização do sistema Pegasus, por exemplo, por mais que forneça ao Estado uma ferramenta extremamente eficiente no que tange à vigilância de possíveis alvos criminosos, também configura um sistema altamente intrusivo. Sua utilização, como vimos no tópico anterior, fere qualquer base principiológica de proteção de dados, bem como o caso prático também não teve a incidência de preocupação por parte do Estado em fornecer qualquer tipo de segurança e transparência quanto ao processamento dos dados obtidos.

Já em relação ao princípio da supremacia do interesse coletivo, explica o Ministro Roberto Barroso:

> "O *interesse público primário desfruta de supremacia porque não é passível de ponderação. Ele é o parâmetro da ponderação. Em suma: o interesse público primário consiste na melhor realização possível, à vista da situação concreta a ser apreciada, da vontade constitucional, dos valores fundamentais que ao intérprete cabe preservar ou promover."*[47]

A relevância deste princípio é frequentemente reforçada pela jurisprudência pátria e pela atuação estatal. Alguns autores entendem, inclusive que a sua obrigatoriedade se justifica em qualquer tipo de ato, porque se trata de uma formalidade necessária para permitir o controle de legalidade dos atos administrativos[48].

No que tange ao interesse público de tratamento de dados pelo Estado, não se questiona que a disponibilização de dados é muito importante para o interesse público. Entretanto, a maneira como o tratamento e a coleta de dados é feita também não pode deixar de ser analisada, e dependendo de quais procedimentos sejam adotados, pode fazer com que o direito à proteção de dados mereça prevalecer.

Fazer com que o interesse público prevaleça em todas as situações significa colocar em risco os direitos fundamentais do homem. Dessa forma, a Administração deve ter muita cautela porque, ao mesmo tempo que a Constituição da República lhe outorgou prerrogativas a fim de atingir o interesse público, a nossa Carta Magna também garantiu aos cidadãos a garantia de observância de seus direitos fundamentais contra o abuso de poder.

Se colocadas essas questões sob análise frente ao Pegasus, o grande ponto a se evidenciar é que, em uma hipótese de admissão desse tipo de *software* invasor, o Estado

---

[47] BARROSO, Luís Roberto. Prefácio à obra Interesses Públicos versus Interesses Privados: desconstruindo o princípio de supremacia do interesse público. 2ª tiragem. Editora Lúmen Júris. Rio de Janeiro, 2007. p. 1299.

[48] DI PIETRO, Maria Sylvia Zanella Direito administrativo / Maria Sylvia Zanella Di Pietro. – 33. ed. – Rio de Janeiro: Forense, 2020. p. 246.

estaria consequentemente legitimando um instrumento que viola frontalmente o direito à privacidade.

Ou seja, sob um olhar sistemático do ordenamento jurídico, a admissão de que deve haver proteção aos direitos da personalidade ligados à proteção de dados não suporta a utilização de um *mallware* invasor de aparelhos pessoais, sem o consentimento e ciência do invadido para utilização de seus dados de maneira indiscriminada e absolutamente desconhecida.

Finalmente, em relação ao princípio da publicidade, este pode ser definido como aquele que "*exige a ampla divulgação dos atos praticados pela Administração Pública, ressalvadas as hipóteses de sigilo previstas em lei*"[49].

A dicotomia entre publicidade e privacidade é evidente, conforme leciona Miriam Wimmer:

> A aparente tensão entre publicidade e privacidade tem sido ocasionalmente suscitada no contexto da necessidade de conciliar regras que impõem ao Estado um elevado grau de transparência quanto às suas atividades e aquelas que exigem que dados pessoais de cidadãos sejam tratados de maneira a preservar a sua intimidade, vida privada, honra e imagem.[50]

Fato é que são muitos os problemas existentes nessa relação de vigilância estatal e direito à privacidade. Dentro dessa temática, cita-se a existência de regras não transparentes de distribuição de serviços públicos, as deficiências dos sistemas computacionais como gatilho para decisões arbitrárias, a distância entre os objetivos declarados e a prática, os sistemas de vigilância baseado na "presunção de culpa", a categorização como uma fonte de estigma social, o risco de discriminação, dentre outros exemplos de problemas[51].

Isso reforça a importância dos debates e discussões para o fortalecimento da aplicação das barreiras e garantias de proteção ao direito à privacidade.

Feitas tais considerações, restou apenas a análise ao princípio da transparência, o qual será abordado em apartado no tópico seguinte, devido à sua especial tensão com o direito à proteção de dados.

---

[49] DI PIETRO, Maria Sylvia Zanella Direito administrativo. 33. ed. – Rio de Janeiro: Forense, 2020.p. 784.
[50] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. *In*: BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 286.
[51] NIKLAS, J.; SZTANDAR-SZTANDERSKA, K.; SZYMIELEWICZ, K. Profiling the unemployed in Poland: Social and political implications of algorithmic decision making (2015). Disponível em: https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf. p. 33-37.

3.4. A tensão entre LGPD e LAI

Quanto ao princípio da transparência, este pode ser entendido como um gênero do qual o princípio da publicidade, o direito à informação e a exigência de motivação são gêneros.

Acerca da motivação - que se refere à externalização as razões de atuação da Administração Pública -, trata-se de um elemento que não acarreta consideráveis tensões com o direito à proteção de dados, mas, na verdade, o fortalece. Isso porque, a transparência do administrador quanto aos motivos e finalidades de sua atuação compatibilizam exatamente com os princípios elencados pela LGPD.

Contudo, no que se refere ao direito à informação, este traz importantes tensões para a sistemática do direito à privacidade.

A Carta Magna elenca algumas passagens relacionadas ao dever do Estado em informar, quais sejam:

> Art. 5º, XXXIII, da Constituição Federal, "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".
>
> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: II - a investidura em cargo ou emprego público depende de aprovação prévia em concurso público de provas ou de provas e títulos, de acordo com a natureza e a complexidade do cargo ou emprego, na forma prevista em lei, ressalvadas as nomeações para cargo em comissão declarado em lei de livre nomeação e exoneração;
>
> Art. 216. § 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

Veja-se, portanto, que o direito à informação é amplamente garantido na Constituição Federal, porém, a maneira como o Estado fornece essa garantia, pode conflitar com a proteção aos dados pessoais dos cidadãos.

Dessa forma, outro desafio que detém o poder público é a compatibilização da Lei Geral de Proteção de Dados com a Lei de Acesso à Informação (LAI - Lei n° 12.527/2011), num constante desafio de encontrar o limiar e o equilíbrio entre o que estabelece ambos os diplomas legais.

Contudo, as próprias legislações em questão carregam em si uma preocupação com essa tensão entre direito à privacidade e a transparência exigidas à atuação do Estado.

A Lei de Acesso à Informação, por exemplo, aborda, em seu artigo 31, inciso II, sobre a necessidade de consentimento para a divulgação de dados, conforme a seguinte redação: "*poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem*".

No mesmo sentido, a LGPD é bem clara ao afirmar que a sua compatibilização com as disposições da LAI deve ser, necessariamente, realizada pelas entidades públicas que efetuarem o tratamento de dados, consoante preconiza o seu art. 23, § 2º: "*o disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)*".

Ademais, a fim de direcionar a atuação estatal, a Lei Geral brasileira indica que a aplicação e o respeito às normas de proteção de dados devem ser sempre pensados com base nas finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas. Transcreve-se os artigos 25 e 26 da referida Lei, para comprovar o cuidado que teve este diploma em tentar conciliar a necessidade de atuação do Estado:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
>
> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

Veja-se que os deveres e funções da Administração Públicas não são esquecidos pela LGPD. Inclusive, as prerrogativas da Lei de Acesso à Informação podem ser reforçadas e complementadas pela própria Lei Geral de Proteção de Dados, como se observa no precedente abaixo:

> MANDADO DE SEGURANÇA - EMPRESA PRIVADA QUE PRETENDE OBTENÇÃO DE DADOS PÚBLICOS DA SEARA CRIMINAL – LEI DE ACESSO A INFORMACAO – LEI GERAL DE PROTEÇÃO DE DADOS – AUSÊNCIA DE QUALQUER HIPÓTESE DE EXCEPCIONALIDADE LEGAL QUE AUTORIZE TAL PROCEDIMENTO – SEGURANÇA DENEGADA. 01. É certo que as informações pessoais em posse do Poder Público tem acesso restrito, independente de sigilo, somente podendo ser acessadas por agentes públicos ou pelos indivíduos a quem os dados se referem, não havendo previsão para que empresas privadas tenham acesso. 02. Conquanto a Lei de Acesso a Informacao e a Lei Geral de Proteção de Dados

> tragam exceções, a hipótese dos autos não se enquadra em qualquer delas. 03. Segurança denegada. (TJ-MS - MS: 14124680620208120000 MS 1412468-06.2020.8.12.0000, Relator: Des. Vladimir Abreu da Silva, Data de Julgamento: 28/04/2021, 4ª Seção Cível, Data de Publicação: 30/04/2021).

No entendimento do referido julgado, a empresa privada que pretendeu a obtenção de dados públicos da seara criminal com base na LAI não obteve seu pleito concedido justamente pelo fato de que, tanto essa legislação, quanto a LGPD não contêm exceção no sentido de fornecer dados registais detidas pelo Estado para agentes civis que não sejam seus titulares ou responsáveis dos titulares, como solicitado pelo impetrante.

Ocorre que, não obstante as ocasiões nas quais o diálogo de fontes entre a Lei n° 12.527/2011 e a Lei n. 13.709/2018 trazerem um resultado evidentemente coordenado, também são comuns as ocasiões que exigem que uma delas deve prevalecer: ou acesso à informação prevaleça, ou a proteção aos dados.

A fim de melhor visualizar tal situação, transcreve-se a ementa abaixo:

> AGRAVO REGIMENTAL. EMBARGOS EM RECURSO DE REVISTA. I - REINTEGRAÇÃO. NULIDADE DO INQUÉRITO ADMINISTRATIVO. NEGATIVA DE EXTRAÇÃO DE CÓPIAS DE DOCUMENTOS CONTENDO DADOS SIGILOSOS SOBRE TERCEIROS. NÃO CONFIGURAÇÃO. AUSÊNCIA DE CONTRARIEDADE À SÚMULA VINCULANTE Nº 14. DIVERGÊNCIA JURISPRUDENCIAL. INCIDÊNCIA DA SÚMULA Nº 296, I, DO TST. 1. Pretensão de declaração de nulidade de inquérito administrativo para apuração de falta grave por empregador sociedade de economia mista, sob o argumento de que é nula a norma interna que obsta a extração de fotocópias de documentos dos autos que guardam informações sigilosas. 2. Nos termos do art. 5º, XXXIII, da Constituição Federal, "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". O dispositivo constitucional assegura o acesso à informação, o que não alcança a circulação de dados sigilosos, como ocorre com a pretensão de extração de fotocópias de documentos com restrição de acesso, mormente quando a obtenção dos dados se destina à produção de defesa no bojo do mesmo processo administrativo em que os documentos estão contidos, hipótese que reforça a desnecessidade de realização de fotocópias de dados sigilosos. Esse é o teor do art. 46 da Lei nº 9.784/99, que, ao assegurar aos interessados a extração de cópias reprográficas do processo administrativo, ressalva os dados e documentos de terceiros protegidos por sigilo. Em que pese à Lei nº 12.527/2011 não se aplicar ao caso em exame, porque posterior aos fatos, seu artigo 6º, III, guia o intérprete acerca do alcance da proteção ao sigilo de que cuida o art. 5º, XXXIII, da Constituição Federal, incumbindo aos órgãos e entidades do poder público - incluídas as sociedades de economia mista, conforme o art. 1º, II, da Lei nº 12.527/2011 - , o dever de assegurar a proteção da informação sigilosa. No caso em exame, a dispensa do Reclamante por justa causa foi precedida de inquérito administrativo na sociedade de economia mista empregadora, no qual se assegurou ao trabalhador o acesso a todos os documentos do procedimento interno, inclusive daqueles que continham dados sigilosos de terceiros, em relação aos quais se obstou apenas a extração de fotocópias. Portanto, não houve restrição ao acesso à informação e tampouco

> ao direito de contraditório e ampla defesa do Reclamante, mas a salvaguarda do sigilo de informações sobre terceiros, que não poderiam circular em fotocópias fora daquele inquérito ou dos setores internos pertinentes do Banco. Ademais, a notícia de que o Reclamante nunca procurou a agência para conhecer do teor do inquérito, donde se extrai que também não requereu a extração de fotocópias, robustece a convicção acerca da integridade formal do procedimento administrativo. Nesse quadro, como foi oportunizado ao Reclamante o acesso a todos os documentos do inquérito administrativo, inclusive no que tange a informações sigilosas sobre terceiros, às quais se restringiu apenas a realização de cópias, não há contrariedade à Súmula Vinculante nº 14, até porque não se examina a regularidade de procedimento investigatório de órgão com competência de polícia judiciária. Outrossim, a inespecificidade do aresto colacionado para o fim de cotejo de teses obsta o conhecimento do recurso de embargos, nos moldes da Súmula nº 296, I, do TST, devendo ser mantida a decisão agravada. Agravo regimental conhecido e desprovido. II - HORAS EXTRAS. CARTÕES DE PONTO NÃO INFIRMADOS POR PROVA EM CONTRÁRIO. AUSÊNCIA DE CONTRARIEDADE À O.J. Nº 233 DA SBDI-1 DO TST. Não infirmados os registros dos cartões de ponto por prova em contrário em nenhum período da relação de emprego em exame, é inaplicável a O.J. nº 233 da SBDI-1, de modo que os embargos não logram conhecimento sob a alegação de contrariedade ao verbete, devendo ser mantido o despacho agravado. Agravo regimental conhecido e desprovido. (TST - AgR-E-RR: 121005120095090242, Relator: Alexandre de Souza Agra Belmonte, Data de Julgamento: 10/08/2017, Subseção I Especializada em Dissídios Individuais, Data de Publicação: DEJT 18/08/2017)

O caso em supra trata-se de uma situação na qual um empregado público foi demitido e houve a abertura de um inquérito administrativo. O Reclamante requereu na justiça o acesso ao respectivo inquérito administrativo que fora aberto, com base na LAI e na garantia constitucional do art. 5º, XXXIII, de acesso à informação.

Contudo, tendo em vista que havia os documentos que continham informações sigilosas sobre terceiros, foi possibilitado ao Reclamante que tivesse acesso ao inquérito administrativo, mas obstou-se a realização de cópias apenas quanto às informações sigilosas.

Assim, o Tribunal Superior do Trabalho entendeu que "*não houve restrição ao acesso à informação e tampouco ao direito de contraditório e ampla defesa do Reclamante, mas a salvaguarda do sigilo de informações sobre terceiros, que não poderiam circular em fotocópias fora daquele inquérito*".

Em conclusão, houve um sopesamento de princípios, haja vista ter-se permitido o acesso ao inquérito por parte do indiciado, em respeito ao direito de acesso à informação e para o exercício do contraditório e ampla defesa, contudo, obstou-se o acesso posterior a documentos que continham dados de terceiros.

Esse é um exemplo claro do diálogo que deve haver entre a LAI e os princípios de proteção de dados.

CONCLUSÃO

O alto fluxo informativo inerente à sociedade atual constitui um elemento gerador de diversas preocupações no que tange à proteção da esfera individual dos indivíduos. É evidente que os direitos à privacidade e à proteção de dados pessoais exigem considerável atenção quando se trata de processamento e compartilhamento de dados, pois referem-se à autodeterminação e constituição da própria personalidade dos cidadãos.

Tal preocupação intensifica-se quando o debate é orientado para a atividade dos entes públicos. Isso porque o Estado possui uma quantidade absurda de dados referentes à sua população e tem o dever de agir de acordo com os princípios da publicidade e da supremacia do interesse público, contudo, não pode deixar de conciliá-los com a esfera de direitos da personalidade de cada indivíduo.

É inconcebível que seja permitido ao Estado atuar em desacordo com as próprias leis que o regem. Contudo, infelizmente não são incomuns os casos nos quais se observa uma atuação estatal que vai além do que seria permitido pelo ordenamento, invadindo esferas de direitos fundamentais que deveriam ter sua guarida garantida, pelo fato de se tratar de um direito fundamental constitucionalmente estabelecido.

O caso do sistema Pegasus desponta como uma preocupante situação, que viola todos os princípios basilares do direito à proteção de dados, como o da finalidade, da necessidade, do livre acesso, da responsabilização e prestação de contas…

O referido *mallware* tem o poder de invadir por completo a esfera de privacidade de qualquer indivíduo que possua aparelho celular com acesso à internet, sem a ciência e o consentimento do portador dos dados. Assim, claramente configurando-se como um sistema ilegal em qualquer nação que possua minimamente um ordenamento de proteção de dados.

Todavia, como sua utilização se deu por parte do Estado, seria correto imputar essa ilegalidade apenas a quem comercializou o programa Pegasus? Qual é a maneira mais adequada de atuação da proteção de dados quando esta já foi violada, frisa-se, pelo próprio Estado?

Não se trata de uma temática simples, pelo contrário. É necessário analisar infinitas nuances, contudo, a sociedade não pode abster-se de compreender que o ser humano é definido e visto socialmente de acordo com seus dados, com suas características, e com as informações que são repassadas sobre ele e, portanto, a má

utilização dos dados pode transformar a vida de uma pessoa completamente, gerando efeitos altamente prejudiciais.

Por isso, não só o estabelecimento de limites à atuação do Estado é essencial, mas também é indispensável que haja o respeito a tais barreiras, especialmente se for levado em consideração que o tratamento de dados em massa é cada vez mais comum e valioso.

Veja-se que, no caso do sistema Pegasus, países que possuem legislações de proteção de dados fizeram uso dessa ferramenta de vigilância, apesar da sua completa incompatibilidade com o direito à privacidade. O exemplo abordado nesta monografia foi o do México, que possui a *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* desde 2010 e, mesmo assim, diversos cidadãos mexicanos tiveram suas intimidades perpassadas, especialmente jornalistas.

O desrespeito à própria legislação protetiva pode gerar consequências ao direito de imprensa, aos princípios da dignidade humana e da liberdade de expressão, dentre tantas outras garantias fundamentais.

Administração possui, necessariamente, o dever de conciliar o princípio de proteção de dados com a sua atuação, sem deixar de respeitar os seus princípios constitucionais explícitos, como o da eficiência e o da publicidade, ou implícitos, como o da supremacia do interesse público.

Nesse sentido, além da necessidade de um controle interno mais eficiente para cumprimento dos direitos legalmente estabelecidos, seria de grande valia que os Estados se preocupassem em unir-se para a elaboração de acordos e contratos internacionais sobre o uso de mecanismos digitais, como o Pegasus, contendo, por exemplo, regras para venda e uso desse tipo de ferramenta.

Uma coisa é certa, os riscos ao direito à privacidade são inúmeros e, tendo em vista o aumento de sistemas e ferramentas para tratamento massivo de dados, a tendência é que essa situação só se intensifique. Assim, a institucionalização de garantias e de previsões legais acerca da proteção aos direitos da personalidade tratados na presente monografia é medida de respeito à própria dignidade da pessoa humana.

O que não se pode é permitir a difusão de *softwares* e aparelhos que invadam a privacidade e a intimidade dos cidadãos, fazendo que a sociedade mitigue a importância ou até perca o entendimento de privacidades, intimidade, segredos, dados pessoais e liberdade.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jacqueline de Souza. **Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós– LGPD**. In: BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 282 – 299.

ALSENOY, B. V.; KINDT, E.; DUMORTIER, J. **Privacy and Data Protection Aspects of e-Government Identity Management**. In: HOF, S. V. D.; GROOTHIUS, M. M. Innovating government: normative, policy and technological dimensions of modern government. Haia: Springer, 2011.

ÁVILA, H. Repensando o "**princípio da supremacia do interesse público sobre o particular**". Revista Eletrônica sobre a Reforma do Estado 11, Salvador, p. 1-30, set.-out.-nov. 2007.

BARROSO, Luís Roberto. **Prefácio à obra Interesses Públicos versus Interesses Privados**: desconstruindo o princípio de supremacia do interesse público. 2ª tiragem. Editora Lúmen Júris. Rio de Janeiro, 2007.

BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLACK, G.; STEVENS, L. "**Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest**". In: Scripted, Vol. 10, Issue 1, April 2013.

BRASIL. **Código Civil.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 24/04/2022.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: https://www.google.com/search?q=cf&oq=cf&aqs=chrome.0.69i59j0i131i433i512j0i512j0i131i433i512j46i131i199i433i465i512j0i131i433i512j0i433i512j0i131i433i512l2j0i512.813j0j7&sourceid=chrome&ie=UTF-8. Acesso em: 24/03/2022.

BRASIL. **Decreto n. 10.046, de 09 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 24/03/2022.

BRASIL. **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: 02/02/2022.

CAVOUKIAN, Ann. **Privacy by Design, The 7 Foundational Principles**: Implementation and Mapping of Fair Information Practices.

COPETTI, Rafael; MIRANDA, Marcel Andreata de. **Informational Self-Determination and Data Protection**: A Critical Analysis of the Brazilian Jurisprudence. Revista de Direito, Governança e Novas Tecnologias, 01 December 2015, Vol.1(1), pp.28-48.

DI PIETRO, Maria Sylvia Zanella **Direito administrativo**. 33. ed. – Rio de Janeiro: Forense, 2020.

DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Joaçaba. V12 N.2, p. 91-108, jul/dez.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

FRAZÃO, Ana (coord.); MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito. Ética, Regulação e Responsabilidade**. São Paulo: Revista dos Tribunais, 2019.

FRIEDMAN, Thomas L. ***How Israel's economy got hooked on selling arms abroad***. **https://www.nytimes.com/1986/12/07/business/how-israel-s-economy-got-hooked-on-selling-arms-abroad.html**. Acesso em: 19/04/2022.

GUERRA, Dolores. **Pegasus e a Ciber Espionagem Israelense no México**. Memo: 2021. Disponível em: https://www.monitordooriente.com/wp-content/uploads/2021/08/PEGASUS-E-A-CIBER-ESPIONAGEM-ISRAELENSE-NO-MEXICO-final-.pdf. Acesso em 09.04.2022.

KNIGHT, Alison. STALLA-BOURDILLON, Sophie. ***Anonymous data v. personal data*** – a false debate: an EU perspective on anonymisation, pseudonymisation and personal

data'. Wisconsin International Law Journal, 2017, 284, 301.

LYON, D. The electronic eye. ***The rise of surveillance society***. Minneapolis: University of Minnesota Press, 1994.

MANTELERO, Alessandro. ***Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection***. Computer law & security review, v. 32, n. 2, p. 238-255, 2016. Disponível em: https://www.researchgate.net/publication/295894703_Personal_data_for_decisional_purposes_in_the_age_of_analytics_From_an_individual_to_a_collective_dimension_of_data_protection

MARQUES, Cláudia Lima. **Superação das antinomias pelo Diálogo das Fontes**: O modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. Revista da Escola Superior da Magistratura de Sergipe (ESMESE), nº 7, 2004.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. São Paulo: Malheiros, 2003

MENDES, Laura Schertel; BIONI, Bruno. **O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira**: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor. Vol. 124. Ano 28. p. 157-180. São Paulo: Editora RT, jul-ago 2019. Disponível em: https://www.academia.edu/42741224/O_regulamento_europeu_de_prote%C3%A7%C3%A3o_de_dados_pessoais_e_a_lei_geral_de_prote%C3%A7%C3%A3o_de_dados_brasileira_mapeando_converg%C3%AAncias_na_dire%C3%A7%C3%A3o_de_um_n%C3%ADvel_de_equival%C3%AAncia.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental / Laura Schertel Mendes. – São Paulo : Saraiva, 2014. – (Série IDP: linha pesquisa acadêmica).

MENDES, Laura Schertel. **Uso de softwares espiões pela polícia: prática legal? Programas permitem controle remoto da câmera e microfone do aparelho**. JOTA, 2015. Disponível em: https://www.academia.edu/42741344/Uso_de_softwares_espio_es_pela_poli_cia_pra_tica_legal. Acesso em: 04.04.2022.

MENDES, Laura Schertel; MATTIUZZO, Marcela. **Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. Revista de Direito Público** – Assunto Especial – Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias.

Vol. 16, nº 90, 2019, p. 39-64, nov-dez 2019. Disponível em: https://www.academia.edu/42741206/Discrimina%C3%A7%C3%A3o_Algor%C3%ADtmica_Conceito_Fundamento_Legal_e_Tipologia.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Diss. Dissertação (Mestrado em Direito) –Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 63-64. Disponível em http://repositorio.unb.br/handle/10482/4782. Acesso em: 09.04.2022.

NIKLAS, J.; SZTANDAR-SZTANDERSKA, K.; SZYMIELEWICZ, K. **Profiling the unemployed in Poland**: Social and political implications of algorithmic decision making (2015). Disponível em: https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf

PASQUALE, Frank. **The Black Box Society**: The secret algorithms that control money and information. Harvard University Press: Cambridge, 2015.

PESCIOTTA, Daniel. ***I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century***. Case Western Reserve Law Review, Vol. 63, Issue 1 (Fall 2012), pp. 187-256.

PINTO, Henrique Alves. **A utilização da inteligência artificial no processo de tomada de decisões:** por uma necessária accountability.RIL Brasília a. 57 n. 225. jan./mar. 2020. p. 43-60.

SARMENTO, Daniel (Org.). **Interesses públicos versus interesses privados: desconstruindo o princípio da supremacia do interesse público**. Rio de Janeiro: Lumen Juris.

TAVARES, Giovanna Milanez. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD**. Rio de Janeiro: Processo, 2022.

UNIÃO FEDERAL. **Emenda Constitucional nº 115 de 10/02/2022**. Disponível em; planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 22.03.2022.

WARREN, Samuel; BRANDEIS, Louis. ***The right to privacy***. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890.

WIMMER, Miriam. **O regime jurídico do tratamento de dados pessoais pelo poder público**. *In*: BIONI, Bruno. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 282 – 299.