Universidade de Brasília - UnB

Faculdade de Direito

MARCIO LUIZ COELHO DE FREITAS

PRIVACIDADE NO DIREITO PENAL E O DILEMA DA VIGILÂNCIA NA ERA DIGITAL: A REGULAÇÃO DA INTERNET COMO INSTRUMENTO DE TUTELA DE DIREITOS FUNDAMENTAIS

Brasília

2022

Universidade de Brasília - UnB

Faculdade de Direito

MARCIO LUIZ COELHO DE FREITAS

PRIVACIDADE NO DIREITO PENAL E O DILEMA DA VIGILÂNCIA NA ERA DIGITAL: A REGULAÇÃO DA INTERNET COMO INSTRUMENTO DE TUTELA DE DIREITOS FUNDAMENTAIS

Tese apresentada como requisito parcial para obtenção do grau de doutor no Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de Brasília.

Orientador: Professor Doutor Alexandre Kehrig Veronese Aguiar

Brasília

2022

MARCIO LUIZ COELHO DE FREITAS

PRIVACIDADE NO DIREITO PENAL E O DILEMA DA VIGILÂNCIA NA ERA DIGITAL: A REGULAÇÃO DA INTERNET COMO INSTRUMENTO DE TUTELA DE DIREITOS FUNDAMENTAIS

Tese apresentada como requisito parcial para obtenção do grau de doutor no Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de Brasília.

Banca Examinadora:

Presidente: _____
Prof. Dr. Alexandre Kehrig Veronese Aguiar

Membro Externo: _____
Prof. Dr. Ney de Barros Bello Filho

Membro Externo: _____
Profa. Dra. Maria Thereza de Assis Moura

Membro Externo: _____
Prof. Dr. André Luis Callegari

Membro Suplente arguidor: _____
Prof. Dr. Othon Lopes

Foi o melhor dos tempos, foi o pior dos tempos. Foi a idade da sabedoria, foi a idade da tolice. Foi a época da fé, foi a época da incredulidade. Foi a estação da luz, foi a estação das trevas. Foi a primavera da esperança, foi o inverno do desespero. Tínhamos tudo diante de nós, não havia nada antes de nós. Todos íamos direto para o céu, todos íamos direto para o outro lado.

Charles Dickens

RESUMO

A presente tese trata de um dos grandes dilemas de nosso tempo: como estabelecer limites adequados para a utilização penal das informações compartilhadas através da internet. Em um mundo onde cada elemento da experiência humana passa a servir de matéria-prima gratuita para alimentar o capitalismo de vigilância, ordem econômica na qual a produção de mercadorias e serviços é subordinada à nova arquitetura global de modificação comportamental, a enorme disseminação de dados e informações pode colocar em risco direitos fundamentais do indivíduo. A persecução penal deve encontrar limites epistemológicos na proteção da privacidade, que não é um direito absoluto, mas é um direito qualificado, cuja relativização e restrição pressupõem uma apreciação concreta das condições fáticas e jurídicas envolvidas na colisão normativa. Por isso, não há como se pensar efetivamente na construção de um estado democrático de direito na era digital sem que se discuta adequadamente de que forma o Estado deve tratar as informações dos indivíduos na persecução penal, buscando um equilíbrio entre a segurança pública e a privacidade. A definição desses limites corresponde à atualização do próprio conceito de Estado de Direito para a era digital, tornando mais efetiva a tutela de direitos fundamentais. Nesse sentido, a solução do problema passa pelo reconhecimento da importância do papel da regulação, compreendida como atividade voltada não só à correção de falhas do mercado, mas também à tutela de direitos fundamentais. Para isso, a tese defende a necessidade de se superar tanto o tecnodeterminismo quanto a visão individualista da privacidade, construída a partir da noção de extensão da propriedade privada (daí se falar em “invasão” ou “violação” da privacidade), adotando-se uma concepção multidimensional e contextual, na qual a privacidade é encarada também em sua dimensão coletiva, relacionada não só à liberdade e à igualdade, mas à própria democracia. Assim, a privacidade no campo penal passa a ser entendida como um limite extrínseco à produção de provas, que encontra na regulação da internet campo profícuo para a sua harmonização com a busca da verdade no processo penal, por meio da técnica de balanceamento e ponderação, feita a partir de uma compreensão contextual aberta aos valores sociais dominantes.

Palavras-chave: surveillance; regulação da internet; direito penal; privacidade contextual.

ABSTRACT

This thesis deals with one of the great dilemmas of our time: how to establish adequate limits for the criminal use of information shared over the internet. In a world where every element of human experience becomes free raw material to feed surveillance capitalism, an economic order in which the production of goods and services is subordinated to the new global architecture of behavioral modification, the enormous dissemination of data and information may jeopardize an individual's fundamental rights. Criminal prosecution must find epistemological limits in the protection of privacy, which is not an absolute right, but a qualified right, whose relativization and restriction presuppose a concrete appreciation of the factual and legal conditions involved in the normative collision. Therefore, there is no way to effectively think about building a democratic state of law in the digital age without properly discussing how the State should treat the information of individuals in criminal prosecution, seeking a balance between public security and privacy. The definition of these limits corresponds to the updating of the very concept of the rule of law for the digital age, making the protection of fundamental rights more effective. In this sense, the solution to the problem involves recognizing the importance of the role of regulation, understood as an activity aimed not only at correcting market failures, but also at protecting fundamental rights. For this, the thesis defends the need to overcome both techno-determinism and the individualistic view of privacy, built from the notion of the extension of private property (hence the terms “invasion” or “violation” of privacy), adopting a multidimensional and contextual conception, in which privacy is also seen in its collective dimension, related not only to freedom and equality, but also to democracy itself. From this, privacy in the criminal field comes to be understood as an extrinsic limit to the admission of evidence, which finds in the regulation of the internet a fruitful field for its harmonization with the search for truth in criminal proceedings, through the technique of balancing and weighting. made from a contextual understanding open to dominant social values.

RESUMEN

Esta tesis aborda uno de los grandes dilemas de nuestro tiempo: cómo establecer límites adecuados para el uso delictivo de la información compartida a través de Internet. En un mundo donde cada elemento de la experiencia humana se convierte en materia prima gratuita para alimentar el capitalismo de vigilancia, un orden económico en el que la producción de bienes y servicios está subordinada a la nueva arquitectura global de modificación del comportamiento, la enorme difusión de datos e información puede poner en peligro derechos fundamentales del individuo. La persecución penal debe encontrar límites epistemológicos en la protección de la privacidad, que no es un derecho absoluto, sino un derecho calificado, cuya relativización y restricción presupone una apreciación concreta de las condiciones de hecho y de derecho involucradas en la colisión normativa. Por lo tanto, no hay forma de pensar efectivamente en la construcción de un estado democrático de derecho en la era digital sin discutir adecuadamente cómo el Estado debe tratar la información de los individuos en la persecución penal, buscando un equilibrio entre la seguridad pública y la privacidad. La definición de estos límites corresponde a la actualización del propio concepto de estado de derecho para la era digital, haciendo más efectiva la protección de los derechos fundamentales. En este sentido, la solución al problema pasa por reconocer la importancia del papel de la regulación, entendida como una actividad encaminada no sólo a corregir fallas de mercado, sino también a proteger derechos fundamentales. Para ello, la tesis defiende la necesidad de superar tanto el tecnodeterminismo como la visión individualista de la privacidad, construida a partir de la noción de extensión de la propiedad privada (de ahí el término “invasión” o “violación” de la privacidad), adoptando una concepción multidimensional y contextual. , en el que la intimidad también es vista en su dimensión colectiva, relacionada no sólo con la libertad y la igualdad, sino también con la propia democracia. A partir de ello, la privacidad en el ámbito penal pasa a ser entendida como un límite extrínseco a la producción de prueba, que encuentra en la regulación de internet un campo fecundo para su armonización con la búsqueda de la verdad en el proceso penal, a través de la técnica de la ponderación. y ponderación, realizada desde una comprensión contextual abierta a los valores sociales dominantes.

SUMÁRIO

1. INTRODUÇÃO

> *O membro do Partido vive, do berço à cova, sob os olhos da Polícia do Pensamento. Mesmo quando está sozinho jamais pode ter certeza do seu isolamento. Onde quer que esteja, dormindo ou acordado, trabalhando ou descansando, no banho ou na cama, pode ser examinado sem aviso e sem saber que o examinam. Nada do que êle faz é indiferente. Suas amizades, seus divertimentos, sua conduta em relação a esposa e aos filhos, a expressão de seu rosto quando está só, as palavras que murmura no sono, e até os movimentos característicos do seu corpo, é tudo ciosamente analisado. É certo que descobrem não apenas as mais minúsculas infrações, como qualquer excentricidade, por pequena que seja, qualquer modificação de hábitos, qualquer maneirismo nervoso que possa ser o sintoma duma luta íntima. Não tem liberdade de escolha em direção alguma.*
> *(1984, George Orwell)*

Em sua célebre obra 1984, George Orwell criou uma ficção totalitária na qual o "Partido", entidade onipresente que personificava o poder e controlava a tudo e a todos por meio de um sistema de vigilância total, estruturou toda a vida social para impedir qualquer possibilidade de pluralidade e pensamento divergente. O Partido não buscava a disciplina dos corpos, mas o poder puro, que se exercia sobre o pensamento. Por isso que, na Oceania de Orwell, "o Partido não se interessa pelo ato em si: é só o pensamento que nos preocupa. Não nos limitamos a destruir os nossos inimigos; nós os transformamos."[1]

Durante muito tempo, a imagem de uma sociedade completamente submetida à vigilância e ao controle encontrou em 1984 sua mais perfeita imagem, sendo apresentada como um futuro distópico. Entretanto, no início do século 21, cada vez mais o exercício de poder do Grande Irmão aparece, senão como uma realidade, pelo menos como uma possibilidade concreta e real. Em outubro de 2010, em uma entrevista sobre o futuro da tecnologia, Eric Schmidt, então CEO da Google, afirmou que

> Com a sua permissão, você nos dá mais informações sobre você, sobre seus amigos e nós podemos melhorar a qualidade de suas buscas. Nós não precisamos sequer que você digite. Nós sabemos onde você está. Sabemos onde você esteve. Nós podemos mais ou menos saber o que você está pensando[2]

A assombrosa semelhança entre as declarações de Schmidt e o mundo retratado em 1984 serve em grande medida como um alerta para a necessidade de se pensar nos limites e

[1] ORWELL, George. **1984**. p. 297

[2] THOMPSON, Derek. **Google's CEO: 'The Laws Are Written by Lobbyists'. Eric Schmidt on the power of lobbyists, a Google "implant", and how China resembles a big business.** Disponível em https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/ (tradução nossa).

possibilidades da privacidade em uma época em que o desenvolvimento tecnológico criou uma sociedade hiperconectada, na qual cada elemento da experiência humana passa a servir de matéria-prima gratuita para alimentar o capitalismo de vigilância, uma ordem econômica cuja lógica de produção de mercadorias e serviços é subordinada à nova arquitetura global de modificação comportamental[3].

Esse é um dado fundamental para a compreensão da forma como vem sendo implantado esse novo modelo de organização social: ao contrário daquele mundo imaginado por Orwell, em que as pessoas seriam vigiadas constantemente, mesmo contra sua vontade, e cederiam seus dados a um governo central forte e onipresente em razão do medo de sanções, atualmente a surveillance, isto é, a vigilância, é extremamente dependente da participação voluntária daqueles que são vigiados, que passam a exercer cada vez mais um papel ativo nesse sistema de vigilância. Como afirma David Lyon[4], não apenas ser observado, mas também observar se tornou um modo de vida, dado que a surveillance atual só se torna possível pelos nossos próprios cliques, curtidas, compartilhamentos, trocas de mensagens de texto, áudios, vídeos, fotos etc.

Outra modificação importante na forma como a vigilância se desenvolve atualmente consiste no fato de que ela não é mais um fenômeno praticado primordialmente por órgãos e agências governamentais, mas conta com forte participação de empresas privadas que têm na obtenção dos dados de seus usuários seu modelo preferencial de negócios. De fato, pelo menos no que diz respeito a dados compartilhados pela internet, tais como os registros de pesquisas feitas em motores de busca, a localização de aparelhos celulares ou de automóveis, postagens e curtidas em redes sociais, por exemplo, o Estado frequentemente só entra no jogo após os dados já terem sido voluntariamente fornecidos pelos usuários às empresas.

As facilidades e conveniências criadas pelas novas tecnologias trouxeram como consequência necessária, mas frequentemente não desejada, o aumento exponencial na capacidade de coleta, armazenamento, análise e disseminação de dados dos usuários, o que coloca em xeque a possibilidade de o indivíduo controlar o acesso ou o fluxo de informações a seu respeito[5]. Nesse contexto, é cada vez mais urgente uma compreensão da privacidade que esteja adaptada à atual realidade.

---

[3] CF ZUBOFF, Shoshana. **The age of surveillance capitalism: The Fight for a Human Future at the New Frontier of Power**, 2019.

[4] Lyon, David. **The culture of surveillance. Watching as a way of life.**Cambridge: Polity Press, 2019.p. 2 e ss.

[5] CF. NISSENBAUM, Helen. **Protecting privacy in a information age: the problem of privacy in public**. Law and Philosophy, 1998. Disponível em SSRN: https://ssrn.com/abstract=139144.

De fato, a privacidade, apesar das enormes controvérsias quanto à sua definição e às diferenças quanto à extensão e amplitude de sua proteção nos diferentes países, é um direito fundamental consagrado em todos os ordenamentos jurídicos modernos e previsto nas mais importantes declarações internacionais de direitos. No Brasil, aliás, foi recentemente aprovada a Proposta de Emenda Constitucional nº 17, que inclui a proteção de dados no rol dos direitos e das garantias fundamentais previstos no art. 5º da Constituição, o qual passou a contar com o inciso LXXIX, dispondo ser "assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

Desde a sua primeira formulação teórica, que remonta a um artigo de Samuel Warren e Louis Brandeis publicado em 1890[6], o direito à privacidade, então concebido como o direito de ser "deixado em paz", teve sua evolução intimamente ligada às mudanças tecnológicas da era industrial. Brandeis e Warren escreveram motivados pela busca de garantir proteção legal contra o uso de máquinas fotográficas portáteis e a publicação de fofocas em jornais impressos, sustentando que a proteção à privacidade através da responsabilização civil seria uma mostra de como o Direito deveria evoluir para responder às mudanças nas circunstâncias sociais. A privacidade, portanto, guarda íntima relação com a tecnologia e com a forma com que a sociedade normatiza o fluxo de informações.

A privacidade é comumente enxergada através de lentes bem estreitas, que nela vislumbram uma construção de base liberal, fundada na subjetividade e na tutela de direitos individuais, sendo frequentemente tratada a partir de metáforas relacionadas a questões ligadas ao aspecto territorial da propriedade privada (daí se falar em "invasão" ou "violação" da privacidade, v.g.) e via de regra é um instituto focado em danos individuais[7]. Entretanto, a proteção da privacidade na era digital não pode ser feita unicamente a partir de uma concepção excessivamente individualista e essencialmente privatística da privacidade. De fato, para se manter um conceito relevante, a privacidade precisa ser compreendida sob uma ótica mais ampla, ligada à proteção do indivíduo contra o abuso do poder, seja por agentes estatais, seja por detentores do poder econômico ou simplesmente contra a intromissão indevida de outras pessoas em assuntos íntimos. A privacidade deve ser compreendida como

[6] WARREN, Samuel D e BRANDEIS, Louis D. **The Right to Privacy**. 1890. Disponível em https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[7] CF. BENNETT, Colin e PARSONS. Christopher. **Privacy and surveillance: the multidisciplinary literature on the capture, use and disclosure of personal information in cyberspace.** In DUTTON, Willian H. **The Oxford handbook of Internet studies.** Oxford: Oxford University Press. 2014. p. . 488.

um conceito em evolução, que tem resistido a todas essas mudanças sociais, evoluindo e se modificando para se adequar às novas realidades[8].

Por isso, em um momento em que a velocidade e amplitude da revolução tecnológica dos meios digitais é cada vez maior, é necessário repensar a forma como o Direito faz a regulação de tais tecnologias, tendo em mente que, como afirma Prosser[9], a busca pela eficiência econômica e correção das falhas de mercado não deve ser o único motivo para justificar a regulação, atividade que também tem um importante papel na criação dos mercados, na implementação de solidariedade social e na proteção de direitos humanos.

No campo do direito penal, a definição dos limites para o exercício do poder persecutório do Estado no mundo digital se torna ainda mais importante, já que os dados coletados pelas empresas na internet podem ser (e serão) objeto de uso secundário na investigação e repressão de crimes. Assim, tem-se que a forma como a privacidade na internet é regulada deve levar em conta também a necessidade de tutela de direitos fundamentais em matéria penal, a fim de que a proteção da privacidade possa manter aderência à realidade social e responder efetiva e adequadamente aos novos problemas relacionados à proteção da pessoa humana.

Na sociedade da informação, os riscos à proteção da privacidade não dizem respeito unicamente a uma mudança de natureza quantitativa, relativa ao expressivo volume de dados coletados e disseminados, mas possui também um aspecto qualitativo, ligado à forma com que tais dados atualmente podem ser tratados e como, a partir da análise e agrupamento desses dados, é possível criar informações novas e relevantes acerca dos grupos e indivíduos. Para que possamos compreender corretamente os desafios da tutela da privacidade na era digital, é preciso ter em mente que o aumento da quantidade de dados disponíveis deve ser conjugado com o vertiginoso aumento na capacidade de processamento de tais dados.

Com a computação passando a mediar a maior parte das relações humanas, o *big data*, processo caracterizado pelo vertiginoso aumento da quantidade de dados coletados e da capacidade de processamento, se tornou o componente fundamental de uma nova lógica de acumulação, o capitalismo informacional, que procura prever e modificar o comportamento humano como forma de gerar receitas e controle de mercado.[10]

---

[8] DEVRIES, Will Thomas. **Protecting Privacy in the Digital Age**, 18 Berkeley Tech, 2003. Disponível em http://scholarship.law.berkeley.edu/btlj/vol18/iss1/19

[9] PROSSER, Tony. **Two visions of regulation.** Paper by Tony Prosser for 'Regulation in the Age of Crisis', University College. Dublin, 2010. Disponível em http://regulation.upf.edu/dublin-10-papers/1H1.pdf

[10] ZUBOFF, Shoshana. ***Big other:* capitalismo de vigilância e perspectivas para uma civilização de informação.** in BRUNO, Fernanda et al. **Tecnopolíticas da vigilância. perspectivas da margem.** São Paulo: Boitempo, 2018. p. 18

O impacto das transformações sociais decorrentes das novas tecnologias de informação e comunicação atinge fortemente a esfera de proteção do indivíduo, já que os contornos e os limites da lei e da regulação face às novas tecnologias não podem ainda ser muito bem estabelecidos e constituem um processo em criação, sendo o resultado da correlação das diversas forças sociais que se contrapõe na defesa da privacidade e da segurança.

Há um evidente descompasso entre a velocidade das mudanças da tecnologia e o tempo do Direito[11]. O caráter disruptivo das novas tecnologias pode atingir severamente aspectos essenciais de ramos do Direito que foram construídos através de gerações, desestabilizando categorias jurídicas fundamentais. A computação em nuvem, por exemplo, desafia a tradicional noção de soberania fundada na aplicação do ordenamento jurídico dentro dos limites territoriais de um país[12]; a inteligência artificial torna menos nítidas as linhas de separação entre agente e objeto e dificulta a utilização de categorias como "vontade livre e consciente"; a informatização de processos judiciais, a utilização de contratos inteligentes e a solução de disputas na internet colocam em xeque a distinção entre a produção de provas e a adjudicação; o crescimento das modernas formas de surveillance, que passou a ser exercida principalmente por empresas e agentes econômicos, faz com que a tradicional distinção público-privado perca muito de sua importância.[13]

É preciso pensar em qual caminho deve a proteção à privacidade seguir para se manter relevante como aspecto de proteção da dignidade humana no mundo contemporâneo. E isso é especialmente verdadeiro quando se pensa na proteção da privacidade em um contexto de segurança pública.

De fato, privacidade e segurança são comumente entendidos como valores que se situam em lados diametralmente opostos, com a proteção da privacidade sendo vista quase como uma ameaça à segurança. Não raro, a proteção da privacidade é tida como um dos piores inimigos da proteção da segurança. Bem ilustrativas dessa visão são as declarações do ex-presidente dos Estados Unidos da América, Barack Obama, que, pouco depois das

---

[11] SVANTESSON, Dan. **The times they are a-changin' (every six months)-- The challenges of regulating developing technologies**. Law papers. disponível em https://www.researchgate.net/publication/27827337

[12] KRISHNAMURTHY, Vivek. **Cloudy with a Conflict of Laws**. The Berkman Klein Center for Internet & Society Research Publication. 2016-03. Disponível em SSRN: https://ssrn.com/abstract=2733350

[13] CF. BROWNSWORD, Roger; SCOTFORD, Eloise, e YEUNG, Karen. **Law, Regulation, and Technology: The Field, Frame, and Focal Questions.** In BROWNSWORD, Roger; SCOTFORD, Eloise, e YEUNG, Karen (orgs). The Oxford Handbook of Law, Regulation and Technology.Oxford: Oxford University Press, 2017. p. 36

revelações de Edward Snowden[14], perguntado sobre o uso governamental de programas de monitoramento de cidadãos, afirmou:

> Eu acho que é importante reconhecer que não se pode ter 100 por cento de segurança e também ter 100 por cento de privacidade e zero de inconveniência. Nós vamos ter que fazer algumas escolhas como sociedade. E o que eu posso dizer é que, na avaliação desses programas, eles fazem a diferença na nossa capacidade de antecipar e evitar possíveis atividades terroristas[15]

Por isso, em uma primeira aproximação, pode até parecer estranho tratar da relação entre privacidade e Direito Penal. Afinal, o Direito Penal é, em última análise, o mais poderoso instrumento de que dispõe o Estado para a tutela de bens jurídicos e para a garantia dos direitos fundamentais, tendo por vocação a tutela de interesses coletivos, ao passo que a privacidade normalmente é vista como um direito especificamente individual, relacionado à possibilidade de o indivíduo ser deixado em paz, livre de interferências da coletividade.

Sob essa ótica, o interesse público em obter informações úteis para prevenir ou reprimir um crime encontraria uma barreira no interesse particular da proteção da intimidade do indivíduo, instalando-se uma clássica colisão entre o individual e o coletivo. A consequência mais evidente dessa forma de encarar a privacidade é que, em matéria de políticas de segurança pública, ela fica relegada a um segundo plano, quase sempre cedendo ante as necessidades coletivas de investigação e repressão de infrações penais, segurança pública, defesa nacional ou segurança do Estado (áreas acerca das quais, por expressa determinação legal - art. 4º, III, - não são aplicáveis as regras da Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais).

Essa visão acaba por reforçar alguns mitos, tais como o de que a privacidade não tem lugar em uma sociedade da informação, com autores chegando mesmo a proclamar a "morte da privacidade na era digital"[16], ou, ainda, a ideia de que a tutela da privacidade no campo da persecução penal só serve para quem quer esconder algo, já que "quem não deve não teme". Por isso, talvez a mais imediata das necessidades quando tratamos da relação entre

---

[14] GREENWALD, Glenn. **NSA collecting phone records of millions of Verizon customers daily.** disponível em https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[15] Tradução nossa. No original: "I think it's important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. We're going to have to make some choices as a society. And what I can say is that in evaluating these programs, they make a difference in our capacity to anticipate and prevent possible terrorist activity."

[16] Há inúmeros autores que sustentam esse ponto de vista, afirmando o fim da privacidade na era digital. Por todos, ver ANDREWS, Lori. **I know who you are and I saw what you did, Social networks and the death of privacy.** 2012.

privacidade e Direito Penal seja buscar compreender corretamente a privacidade no contexto da atual sociedade da informação, fazendo uma espécie de "ortopedia" dos institutos jurídicos e conceitos a ela relacionados para que seja possível desfazer alguns desses mitos.

Especificamente no campo do Direito Penal, a imersão das pessoas no ciberespaço e a ascensão do *big data* possibilitam que cada vez mais informações detalhadas passem a estar disponíveis para os encarregados das atividades de policiamento e persecução penal. A conjugação de fatores como a progressiva difusão das tecnologias de mineração de dados na rede mundial de computadores, o aumento da utilização de informações agrupadas em novas bases de dados e a análise preditiva, aliada à utilização de instrumentos de reconhecimento biométrico ou facial, fará com que cada vez menos as atividades de policiamento e investigação tenham que ser feitas a partir da observação direta e passem a ser feitas a partir da análise de dados agrupados estatisticamente, que orientarão onde, quando e como as autoridades policiais devem agir para combater a prática de crimes[17].

Tradicionalmente, em um mundo em que as evidências são coletadas analogicamente, quando se discute a delimitação do campo legítimo de atuação do poder público na persecução penal, buscando estabelecer-se o espaço juridicamente protegido do indivíduo, a principal questão a ser definida é se o Estado poderia coletar determinadas provas contra o indivíduo sem autorização judicial. Exemplo marcante disso é o reconhecimento da necessidade de proteção do domicílio como um direito protegido pela cláusula da reserva de jurisdição e à necessidade de que a situação de flagrância, que excepciona a necessidade de mandado judicial, seja amparada em justa causa existente antes da entrada das forças policiais no domicílio[18].

Na atual realidade, entretanto, não faz sentido que a ênfase da proteção à privacidade se concentre nas restrições à coleta da informação, já que, no mais das vezes, ela é disseminada voluntariamente pelo próprio titular do direito que, com um clique, autoriza a realização da coleta, tratamento e compartilhamento de dados sensíveis, simplesmente se limitando a aceitar os termos de serviço de provedores, aplicativos e serviços fornecidos via *web*. Por isso, para poder equacionar corretamente esse balanceamento entre privacidade digital e segurança pública, é cada vez mais necessário o desenvolvimento não só de uma

[17] FERGUSON, Andrew Guthrie. **The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement.** 2017, p. 11

[18] O Supremo Tribunal Federal definiu, em repercussão geral, que o ingresso forçado em residência sem mandado judicial apenas se revela legítimo – a qualquer hora do dia, inclusive durante o período noturno – quando amparado em fundadas razões, devidamente justificadas pelas circunstâncias do caso concreto, que indiquem estar ocorrendo, no interior da casa, situação de flagrante delito (RE n. 603.616/RO, Rel. Ministro Gilmar Mendes, DJe 8/10/2010).

teoria constitucionalmente adequada sobre o acesso e a utilização de dados em poder de terceiros (algo como a *third party doctrine* do direito norte americano), mas também é necessário que a privacidade, como direito fundamental, seja corretamente compreendida e valorada, de modo a permitir que, quando em colisão com outros direitos fundamentais, especialmente na área da segurança pública, o resultado do balanceamento não deixe o indivíduo desprotegido.

A extensão e intensidade da utilização das novas tecnologias tornaram a comunicação muito mais eficiente, mas também deixam os cidadãos mais vulneráveis. Os limites historicamente construídos para a atuação persecutória estatal em muitas situações parecem não mais responderem adequadamente às necessidades atuais.

Com efeito, o marco legal atual não deixa dúvidas de que, para que a polícia e o Ministério Público possam obter e utilizar validamente como prova documentos guardados no local de trabalho de um indivíduo investigado, é necessária a obtenção de autorização judicial específica, concedida após a demonstração da existência de indícios de autoria e prova suficiente de materialidade. Entretanto, quando se trata, por exemplo, de dados disponibilizados em redes sociais, mesmo que fechadas, os requisitos não são claros. O mesmo se diga da possibilidade de requisição por parte do Ministério Público ou da autoridade policial de dados cadastrais ou de conexão em posse de operadoras de telefonia e provedores de internet, questões objeto de intensa discussão no âmbito do Supremo Tribunal Federal (STF) e no Superior Tribunal de Justiça (STJ).

A resposta, entretanto, não tem sido uniforme, e, muitas vezes, sequer a questão da privacidade é colocada de modo claro e expresso no debate, que fica girando unicamente ao redor da necessidade de se garantir maior efetividade às investigações e à segurança pública, tutelando-se prioritariamente o interesse público em evitar ou punir crimes graves sobre o interesse "meramente individual" de tutela da privacidade do investigado.

Isso evidencia a necessidade de que, em um contexto de hiperconvergência tecnológica, onde a interconexão de várias fontes de dados pessoais e a ampliação da capacidade de processamento tornaram a obtenção de processamento secundário de dados algo corriqueiro, se busque uma correta compreensão do que é privacidade digital e qual sua importância no mundo contemporâneo, de forma a permitir que se encontre um equilíbrio mais adequado entre privacidade e segurança pública, dois valores fundamentais para uma sociedade que se pretenda democrática.

É preciso, portanto, discutir de que forma é possível, em uma sociedade democrática, compatibilizar a segurança pública e a privacidade, ante as novas tecnologias de informação e

comunicação, tentando resguardar os usos legítimos e necessários e ao mesmo tempo impedindo uma intervenção excessiva. Em suma, é preciso construir respostas sobre quais são os limites e as possibilidades da utilização, no campo criminal, de dados coletados, compartilhados, processados, analisados e categorizados para efeito de limitar direitos fundamentais dos cidadãos.

Por isso, pensar o Direito Penal na era digital é uma tarefa que não envolve apenas a análise de crimes virtuais ou crimes cometidos através da internet. Tampouco se limita a discutir a produção de provas nos meios digitais, mas pressupõe que seja corretamente enfrentado o enorme desafio teórico de se pensar na relação que o indivíduo deve manter com o Estado no mundo atual, restabelecendo-se, à luz da nova realidade de regulação da informação, os marcos que delimitam as barreiras de proteção do indivíduo contra a ação persecutória estatal.

A definição de critérios teóricos que permitam o estabelecimento de limites e possibilidades para a ação governamental nesse campo é especialmente importante quando se nota que estamos vivendo um momento no qual o direito penal, por uma grande variedade de fatores[19], passa a ser visto como o meio por excelência de gestão de riscos sociais, perdendo sua função clássica de *ultima ratio* para ser *prima* ou *sola ratio*. Assim, os princípios clássicos do direito penal, estabelecidos como legado do iluminismo[20], precisam de uma releitura para que possam manter sua importância e eficácia na era digital.

Nessas condições, a questão mais importante para o balizamento do campo legítimo de atuação estatal deixa de ser a relativa aos limites para a coleta das informações pessoais e passa a ser a relativa aos limites para a sua utilização após o compartilhamento, quando a informação coletada pode ser compartilhada com outras empresas e órgãos estatais, onde estará sujeita a agrupamento, classificação e processamento. A questão mais relevante, portanto, deixa de ser a obtenção do dado e passa a ser a relativa ao seu uso secundário[21].

A presente tese objetiva fazer uma análise dos limites e possibilidades da utilização de dados pessoais disponíveis na internet pelos órgãos estatais encarregados da persecução penal, discutindo o papel que a regulação da privacidade digital pode ter na proteção de direitos fundamentais em matéria penal.

---

[19] CF. SANCHEZ, Jesus Maria Siva. **A expansão do Direito Penal.** 2a. edição. São Paulo: Revista dos Tribunais. p. 24 e ss.

[20] FERRAJOLI, Luigi. **Direito e razão. Teoria do garantismo penal.** p. 17

[21] ETZIONI, Amitai, **A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational**, Brooklin Law Review, Vol. 80. 2015. disponível em http://brooklynworks.brooklaw.edu/blr/vol80/iss4/2

Trata-se da introdução da regulação como elemento importante no cada vez mais intenso debate que contrapõe de um lado a privacidade e, de outro, a necessidade de o Estado obter elementos de inteligência e meios de provas necessários para prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, o que cada vez mais pressupõe a possibilidade de circulação desses dados entre os diversos órgãos governamentais[22].

Neste ponto, cumpre ressaltar que não se trata aqui unicamente de realçar a importância da proteção da privacidade contra a surveillance governamental, mas, antes, cuida-se de definir os contornos adequados para a proteção do indivíduo contra a persecução penal na atual configuração social e ante as modificações trazidas pelas novas tecnologias de informação e comunicação. Acreditamos que o próprio instituto da privacidade, para se manter relevante, necessita de uma releitura a fim de que possua capacidade de rendimento e possa responder adequadamente à finalidade de proteção da dignidade da pessoa humana para a qual ele foi concebido.

De fato, os limites da tutela da privacidade devem ser estipulados a partir de uma análise regulatória que leve em consideração todas as possibilidades de utilização, transferência e processamento das informações recolhidas, posto que, uma vez autorizado o processamento da informação, ainda que apenas com uma empresa privada para efeitos comerciais, dificilmente será possível garantir que sua utilização se restrinja a esse campo. A uma, porque as próprias empresas de tecnologia promovem a circulação das informações, comercializando-as com terceiros (*data brokers*). Além disso, uma vez que a informação esteja disponível para efeitos civis, dificilmente os detentores poderão deixar de fornecê-las às autoridades que pretendam utilizá-la para efeitos penais. Daí porque optamos por centrar nossa análise na regulação da privacidade digital, uma vez que é a partir da definição dos limites e possibilidades da coleta de dados pessoais que será possível construir um modelo de utilização penal dos dados adequado à tutela dos direitos fundamentais do indivíduo. A dizer: a regulação da coleta e o tratamento de dados pessoais deve levar em conta também os efeitos sobre a persecução penal, de modo a buscar atingir o melhor equilíbrio entre os direitos fundamentais do indivíduo e os interesses da sociedade.

[22] A distinção entre dados de inteligência e meios de prova remete aqui à distinção entre meios de prova (isto é, elementos que poderão ser submetidos à análise cruzada pelas partes e podem ser utilizados autonomamente como fundamento de decisões condenatórias em matéria penal) e meios de investigação (elementos que se prestam unicamente e orientar o sentido de evolução de uma investigação, já que configuram indícios que não podem ser utilizados para dar sustentação a uma sentença condenatória). Sobre o tema, ver LOPES JUNIOR, Aury; GLOECKNER, Ricardo Jacobsen. **Investigação Preliminar no Processo Penal**. 5ª ed. São Paulo: Saraiva, 2013, p. 322-323.

De outro lado, deve-se ressaltar que, na era digital, não são somente a pervasividade e a vigilância inerentes às novas tecnologias que representam risco à privacidade. Há também um enorme risco na eventual disseminação da percepção de que a privacidade, especialmente quando pensada em um contexto de limitação aos poderes estatais, possa servir de anteparo para a prática de crimes ou de comportamentos que coloquem em risco bens jurídicos tutelados pelo ordenamento jurídico. Uma tal ideia, a longo prazo, fatalmente levaria a privacidade a perder seu nível de proteção jurídica que o ordenamento lhe confere.

A redefinição dos contornos da privacidade é relevante não só como medida de proteção ao indivíduo, mas também como medida de proteção da coletividade, já que é preciso se pensar em uma forma de regulação da privacidade que a compatibilize com o interesse público legítimo de garantir segurança às pessoas, permitindo que o Estado possa desincumbir-se de seu papel de garante dos direitos fundamentais, tarefa para a qual o direito penal tem um papel de fundamental importância.

Por isso, em uma sociedade que se pretenda democrática, nem não é possível pensar-se na privacidade como um direito de segunda categoria, que sempre sucumbiria a qualquer interesse público a ela contraposto. Tampouco é admissível se pensar na privacidade como um direito absoluto, que se funcione como um biombo protegendo a possibilidade da prática de crimes. A privacidade deve ser compreendida em um contexto de necessidade de compatibilização do individual e do coletivo, sob pena de tornar-se realmente obsoleta e perder utilidade em um mundo marcado pelo tráfego de informações e onde os riscos crescentes aumentam exponencialmente as demandas por mais segurança.

Assim, um estudo que tem como objeto principal a discussão dos limites e possibilidades da utilização de dados pessoais obtidos na internet para efeitos penais deve necessariamente centrar-se na análise da construção das regras relativas ao tratamento dado às informações sobre os indivíduos.

Os limites e possibilidades da coleta, armazenamento, análise e compartilhamento das informações são objetos específicos da regulação da política de dados pessoais na internet, e a forma como o Direito trata a informação é elemento chave para o equilíbrio das relações de poder, por isso que não há como se pensar efetivamente na construção de um estado democrático de direito na era digital sem que se discuta adequadamente de que forma o Estado deve tratar as informações dos indivíduos para efeito de persecução penal. Compreendida dessa forma, a definição de tais limites para a atuação estatal, especialmente em matéria penal, corresponde na verdade a uma atualização do próprio conceito de estado de direito apropriado para a era digital.

No presente trabalho, procuraremos, a partir de contribuições das teorias regulatórias centradas no interesse público, compreender o impacto das novas tecnologias de informação e comunicação, em especial da internet, sobre a atividade estatal de persecução penal. O que se busca é, a partir de uma concepção ampla de regulação da internet (e das novas tecnologias de informação e comunicação que a ela são ligadas), compreender como é possível ao Estado regulador compatibilizar a busca pela tutela do interesse público no ciberespaço com a liberdade e a generatividade da internet[23], isto é, com sua abertura para a inovação.

Vale notar que, apesar da ampla projeção que a proteção da privacidade na internet tem assumido no que diz respeito às relações civis, na área penal esse é um campo ainda bastante aberto, sendo certo que há diferenças marcantes e fundamentais entre as duas abordagens a justificar a necessidade do aprofundamento de pesquisas relacionadas à privacidade no campo penal.

De fato, em se tratando de relações civis, à privacidade dos usuários se contrapõem interesses financeiros das empresas fornecedoras de serviços pela internet ou pelo menos uma maior comodidade na prestação do serviço, por isso que, nessa seara, o aspecto econômico da relação ganha proeminência, de modo que, na regulação das relações civis e comerciais, a privacidade é tida como um direito posto e praticamente todo o ônus argumentativo fica a cargo de quem pretende restringi-la. Por outro lado, quando a restrição à privacidade se dá para assegurar o acesso pelo Estado a dados necessários para a tutela de outros interesses públicos relevantes, que também assumem o caráter de substrato de direitos fundamentais, como a segurança, a ponderação muda completamente, de forma que quase sempre a balança pende a favor desta última[24].

A presente tese visa a buscar teorias que permitam compreender o fenômeno da ampla disseminação das novas tecnologias na atualidade para identificar parâmetros que possibilitem estabelecer os limites e possibilidades de atuação legítima do poder público na obtenção e no processamento dos dados digitais para efeitos penais, demarcando o campo possível do exercício da liberdade individual. Para tanto, buscaremos compreender os limites e a possibilidade da regulação da internet, não só em seu aspecto jurídico, mas também do ponto

[23] O termo foi cunhado por Jonathan Zittrain, numa alusão ao sétimo estágio na teoria de desenvolvimento psicossocial de Erik Erikson, para se referir à possibilidade de que desenvolvedores sem qualquer relação com os responsáveis pela rede ou com provedores de acesso possam oferecer aos consumidores novos produtos e serviços. CF. ZITTRAIN, Jonathan. **The Future of the Internet and How to Stop It. The Future of the Internet - And How to Stop It.** New HAven: Yale University Press, 2008. Disponível em: http://ssrn.com/abstract=1125949

[24] CF. SOLOVE, Daniel J. **Nothing to hide. The false tradeoff between privacy and security.** New Haven: Yale University Press, 2011

de vista técnico, tendo presente a existência de uma inter-relação dialética entre as quatro forças regulatórias que atuam no campo da internet: a lei, o mercado, as normas sociais e a arquitetura. Em razão disso, as teses de Lawrence Lessig[25] e Andrew Murray[26] acerca da regulação da internet apresentam-se como pontos de partida fundamentais sobre os quais irá se desenvolver a investigação.

Além disso, buscaremos compreender o fenômeno regulatório a partir das teorias de Julia Black[27] e Tony Prosser[28], que adotam uma aproximação procedimental da regulação, mas com atenção a aspectos materiais relacionados ao interesse público, além de defenderem uma visão mais ampla da regulação, que deixa de gravitar exclusivamente na órbita do Estado (através dos órgãos da administração ou de agências reguladoras autônomas) e passa a incluir a autorregulação, a corregulação e até mesmo a regulação por organizações privadas, elemento essencial para a correta compreensão da regulabilidade e governança da internet, ainda fortemente marcada pela autorregulação.

Assim entendido, o escopo da regulação deixa de ser apenas a correção de falhas de mercado e a busca pela eficiência econômica, e passa a incluir vários outros objetivos inerentes ao interesse público, inclusive no que toca à implementação de direitos fundamentais, o que se mostra importante para a compreensão e o tratamento das questões relacionadas à tutela da segurança pública.

Por outro lado, para a compreensão da privacidade digital e sua reformulação, faremos uma análise da evolução da ideia de privacidade, a partir dos trabalhos de Hannah Arendt e Jürgen Habermas sobre a distinção entre público e privado, para, em seguida, tratar da readequação do instituto da proteção à privacidade na era digital, a partir das teorias de Helen Nissenbaum[29] e Daniel Solove[30], que sustentam uma visão complexa da privacidade, não como mero controle de acesso ou do conteúdo de informações particulares do indivíduo. Dessa forma, a privacidade passa a ser vista não somente como um interesse individual,

---

[25] LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0,** New York: Basic Books, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[26] MURRAY, Andrew. **Nodes and gravity in virtual space.**

[27] BLACK, Julia. **Critical Reflections on Regulation**, LSE Centre for the Analysis of Risk and Regulation Discussion Paper 4, 2002. Disponível em http://www.lse.ac.uk/accounting/CARR/pdf/DPs/Disspaper4.pdf.

[28] PROSSER, Tony. **Two visions of regulation.** Paper by Tony Prosser for 'Regulation in the Age of Crisis', University College. Dublin, 2010. Disponível em http://regulation.upf.edu/dublin-10-papers/1H1.pdf e PROSSER, Tony. **Theorising Utility Regulation.** Heinonline, 62 Mod. L. Rev. 196. 1999

[29] NISSENBAUM, Helen. **Privacy in context. Technology, policy and the integrity of social life.** Stanford: Stanford Law Book, 2010. Ainda NISSENBAUM, Helen. **Protecting privacy in a information age: the problem of privacy in public**. Law and Philosophy, 1998. Disponível em https://ssrn.com/abstract=139144.

[30] SOLOVE, Daniel J. **Nothingo to hide. The false tradeoff between privacy and security.** New Haven: Yale University Press, 2011.

especificamente vinculado àquela pessoa que a exerce, mas como um valor social, que diz respeito aos limites de proteção dos direitos do indivíduo contra a arbitrariedade e tirania. Essa perspectiva fornecerá maior capacidade de rendimento à análise das colisões entre a segurança pública e a privacidade digital.

Por fim, buscaremos compreender os impactos da moderna surveillance digital, ou *dataveillance*, sobre o direito penal e como a privacidade pode ser compreendida como um limite epistemológico à produção da prova. Para trabalharmos com ideia de busca de harmonização e balanceamento na colisão entre privacidade digital e segurança pública, buscando demarcar as possibilidades de exercício legítimo da *surveillance digital* e a utilização de dados pessoais para efeitos penais, utilizaremos a teoria do balanceamento e da ponderação de Robert Alexy conjugada com a privacidade contextual de Nissembaum.

1.1. PROBLEMA E HIPÓTESE

O problema central a ser enfrentado pela presente pesquisa é o de saber se, na regulação da internet, a adoção de uma abordagem multidimensional da privacidade, adequada à complexidade de seu objeto, pode servir como instrumento efetivo para a tutela de direitos fundamentais, possibilitando que a análise das colisões entre privacidade e segurança pública possam ser solucionadas de modo mais adequado, possibilitando que os direitos fundamentais dos investigados sejam respeitados e protegidos na maior medida possível, ao mesmo tempo em que se busca maximizar a eficiência e eficácia do uso das novas tecnologias como instrumentos de obtenção de prova em matéria penal. Em outras palavras, o que se busca é saber como resolver os problemas relacionados aos limites entre a privacidade e a atuação estatal voltada à segurança pública no atual contexto de coleta, compartilhamento e processamento maciço de dados.

A hipótese inicial de trabalho é de que a correta identificação dos pressupostos fáticos e epistêmicos da colisão entre a privacidade e a segurança, aliada à criação de um quadro teórico a partir da teoria da privacidade contextual de Nissembaum e à utilização de um conceito amplo de regulação, permitirão imprimir maior solidez às soluções das colisões normativas, delimitando o campo possível de atuação estatal quanto aos dados compartilhados, voluntariamente ou não, no ciberespaço, suficientemente flexível para se adequar às diferentes configurações de regulação e governança na internet.

1.2 SOBRE O MÉTODO

A regulação da internet e a tutela da privacidade na era digital não podem ser tidos como temas propriamente novos, sendo certo que muita literatura e pesquisas sobre o tema têm sido produzidas. Há inúmeros estudos acerca da proteção ao consumidor e ao usuário dos serviços digitais, da governança da internet e mesmo acerca da vigilância sobre os cidadãos. Entretanto, especialmente no Brasil, poucas são as iniciativas de associar uma abordagem técno-regulatória das novas tecnologias de informação e comunicação com a definição de limites para a atuação estatal em matéria penal.

Essa perspectiva do problema pressupõe a existência de acordos semânticos muito bem delimitados, já que envolve temas ainda muito abertos tanto no campo do Direito Regulatório, quanto no Direito Penal e Constitucional. De fato, a presente tese procura se inscrever exatamente na confluência destes três ramos do Direito, por isso é preciso estar sempre atento ao risco de utilização de termos e conceitos muito próprios de um ramo que não necessariamente carrega a mesma carga de significado quando transposto para outra área. Por isso, pensamos ser necessária uma abordagem que principie sempre pelo esclarecimento do sentido e do alcance dos termos utilizados e dos institutos jurídicos que servirão de base para a realização das análises.

Assim, uma vez que os objetivos perseguidos serão buscados principalmente através por intermédio da análise de institutos jurídicos relacionados a direitos fundamentais, especialmente a privacidade, e uma vez que este instituto deverá ser objeto de uma releitura que garanta sua capacidade de rendimento como instituto jurídico na era digital, tem-se que o presente estudo constitui uma pesquisa de cunho eminentemente dogmático.

Neste ponto, visando a afastar algumas dúvidas que a expressão possa suscitar, cabe esclarecer que por dogmática jurídica não se faz aqui qualquer alusão a uma visão positivista radical, que vê na lei todo o direito e que tem as normas como verdades absolutas com as quais deve trabalhar o jurista. Na verdade, o caráter dogmático do Direito não tem relação com o conteúdo ou com a exaustividade das normas, mas com a inevitabilidade dos pontos de partida (isto é, com a constatação da existência de normas que vinculam o operador do Direito). Como afirma João Maurício Adeodato[31], a inquestionabilidade dos pontos de partida

[31] ADEODATO, João Maurício. **Ética e retórica: para uma teoria da dogmática jurídica.** 4. ed. São Paulo: Saraiva, 2009, p. 151

> [...] não significa que os dogmas jurídicos sejam interpretações estáticas da conduta social, uma vez que eles precisam ser constantemente revistos a fim de acompanhar a mutabilidade inerente àquela conduta. A dogmática jurídica consiste justamente na sistematização e no manejo das regras que garantem que esses processos de revisão e atualização permanecerão dentro dos limites fixados pelas próprias normas jurídicas, estabelecendo modos interpretativos e integradores para a adaptação da norma ao fato.

Por outro lado, cabe esclarecer que a dogmática é aqui entendida segundo a concepção de Alexy[32], para quem a dogmática jurídica (isto é, a "Ciência do Direito" ou a "Ciência jurídica") em grande medida é uma tentativa de se dar uma resposta racionalmente fundamentada a questões axiológicas que foram deixadas em aberto pelas normas existentes.

Alexy entende que a dogmática jurídica é uma disciplina pluridimensional, de modo que a Ciência do Direito, em seu sentido próprio e restrito, teria três dimensões[33]: a dimensão *lógico-analítica*, em que são analisadas as estruturas lógicas do Direito, desde a análise dos conceitos elementares, passando por construções jurídicas até o exame das estruturas do sistema jurídico; a dimensão *descritiva-empírica*, que diz respeito ao conhecimento do direito positivo válido, bem como à descrição e ao prognóstico da práxis dos tribunais; e, finalmente, a dimensão *normativa-prática*, em que se busca elaborar propostas para a solução dos casos jurídicos problemáticos, a fim de determinar, a partir do direito válido, qual a decisão correta a ser tomada em um caso concreto[34].

Vale ressaltar que para Alexy essas três dimensões da dogmática devem ser combinadas se o Direito quiser cumprir sua função prática, qual seja, a de responder, em face de um caso real ou hipotético, aquilo que *deve ser*, posto que "combinar as três dimensões é uma condição necessária de racionalidade da ciência jurídica como disciplina prática"[35].

Isto não obstante, no presente trabalho, em razão dos objetivos propostos, o enfoque central será na dimensão lógico-analítica, já que a clareza analítico-conceitual é uma pré-condição para a racionalidade de qualquer ciência, o que é especialmente verdadeiro nas ciências humanas normativas, como o Direito. Tal orientação ficará evidente no curso da presente pesquisa, onde a definição, o desenvolvimento e a sistematização de conceitos-

---

[32] Cf. ALEXY, Robert. **Teoria dos Direitos fundamentais.** P. 33 e SS. Ver também, do mesmo autor, **Teoria da argumentação jurídica**, p. 240.

[33] De notar que a tese de Alexy diferencia-se da tese da tridimensionalidade de Miguel Reale porque, enquanto para Reale, a tridimensionalidade é ontológica (o Direito *é* tridimensional), para Alexy a tridimensionalidade é epistemológica, ou seja, o direito é um fenômeno uno, que deve ser estudado a partir dessas três dimensões (Cf. GUERRA FILHO, 1995, p. 152)

[34] ALEXY, Robert, **Teoria da argumentação jurídica**, São Paulo: Landy, 2001. p. 240.

[35] ALEXY, Robert. **Teoria dos Direitos fundamentais**. São Paulo: Malheiros, 2008, p. 37

chave, como os de internet, regulação, *big data*, privacidade, governança, tecnologias de informação e comunicação e internet, ocuparão lugar central.

Não se desconhece as críticas que o método analítico sofreu, especialmente no campo do direito penal, onde já se acusou a dogmática jurídico-penal de dificultar a resolução dos problemas reais e concretos, privilegiando um exagerado academicismo. Nesse sentido é que Gimbernat Ordeig[36], relembra a crítica de Richard Schmid à dogmática alemã, que teria deixado de compreender o crime como um problema humano passou a vê-lo unicamente como um problema jurídico, de subsução das condutas às normas, de modo que "[...] a disciplina do direito penal se cultivou como *l'art pour l'art*, sendo elaborada com toda classe de sutilezas"[37] afastando-se cotidiano, do mundo concreto e real no qual se desenvolvem os problemas humanos.

Ocorre, entretanto, que mesmo a despeito das limitações inerentes ao método analítico, sua observância nos parece fundamental na construção de uma teoria jurídica que pretenda contribuir para afastar decisionismos e irracionalidades. Com efeito, como afirma Alexy[38],

> Sem uma compreensão sistemático-conceitual, a Ciência do Direito não é viável como disciplina racional. A medida de racionalidade do Direito depende em grande parte do nível alcançado pela dimensão analítica. Sem clareza analítica, nem mesmo seriam possíveis enunciados precisos e fundamentados sobre a interação das três dimensões. Seria impossível falar de um controle racional das valorações indispensáveis à Ciência do Direito e de uma aplicação metodologicamente controlada do saber empírico. Se há algo que pode livrar ao menos um pouco a ciência dos direitos fundamentais da retórica política e das idas e vindas das lutas ideológicas é o trabalho na dimensão analítica. Se acrescentarmos que na dimensão analítica da Ciência do Direito são possíveis conhecimentos que, em primeiro lugar, não podem ser substituídos por conhecimentos de nenhuma outra ciência e que, em segundo lugar, estão entre os conhecimentos mais seguros da Ciência do Direito, há, então, motivos suficientes para se designar e praticar a análise sistemático-conceitual do direito como *opus proprium* da Ciência do Direito.

[36] GIMBERNAT ORDEIG, Enrique **¿Tiene un futuro la dogmatica juridicopenal?** Madrid: Editorial Civitas,1984. Disponível em https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080521_84.pdf

[37] Tradução nossa. No original: "la disciplina del Derecho penal se cultivó l'art pour l'art, por así decir, siendo elaborada con toda clase de sutilezas jurídicas"

[38] ALEXY, Robert. **Teoria dos Direitos fundamentais.** P. 49.

Referindo-se especificamente ao campo do direito penal, Gimbernat Ordeig[39] ressalta a importância da dogmática como meio de se afastar o risco de que as decisões judiciais se transformem em uma loteria, afirmando que

> A dogmática jurídico-penal, ao assinalar limites e definir conceitos, torna possível uma aplicação segura e calculável do Direito penal, e o afasta da irracionalidade, da arbitrariedade e da improvisação. Quanto mais pobre seja o desenvolvimento de uma dogmática, tanto mais imprevisíveis serão as decisões dos tribunais... E quanto menor seja o desenvolvimento dogmático, tanto mais cresce essa loteria, até chegar a uma situação de aplicação caótica e sem rumo de um Direito penal [...] Onde estão em jogo paixões humanas — e em que processo penal não ocorre assim —, a fonte mais turva do conhecimento é um sentimento jurídico não articulável conceitualmente.[40]

Por isso, especialmente quando se tem em mente as dificuldades inerentes à definição de limites para uma atuação estatal relativamente nova, sobre a qual inexistem consensos, parece essencial que se inicie pela abordagem analítica dos conceitos e de suas inter-relações, de modo a deixar claro sobre o que estamos falando.

O lugar de destaque conferido à dimensão analítica no curso do presente trabalho, todavia, não quer significar que aqui se pretenda unicamente fazer um exercício de abstração analítica. Com efeito, até em razão da multidimensionalidade da dogmática, nenhuma análise pode ser correta se não enfocar também as dimensões empírica e normativa. Daí porque, visando a afastar a possibilidade de incorrer-se em um formalismo exacerbado, fruto de uma análise conceitual que acabe gerando um distanciamento da realidade, a pesquisa também se deterá na dimensão empírica da dogmática, por meio da busca da forma como a jurisprudência vem tratando alguns dos temas analisados no presente trabalho.

Nesse sentido, serão analisadas decisões recentes do Supremo Tribunal Federal acerca da tutela da privacidade em matéria penal, com especial destaque para as decisões proferidas na ADI 5642, na qual a Associação Nacional das Operadoras de Celulares (ACEL) questiona a constitucionalidade do art. 11 da Lei 13.344/2016, que dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas,

---

[39] Apud ROXIN, Claus. **Derecho Penal**. **Parte general.** Fundamentos. La estructura de la teoría del delito. Madrid: Civitas, 1997. p. 207.

[40] Tradução nossa. No original: “La dogmática jurídicopenal, al señalar límites y definir conceptos, hace posible una aplicación segura y calculable del Derecho penal, y lo sustrae a la irracionalidad, a la arbitrariedad y a la improvisación. Cuanto más pobre sea el desarrollo de una dogmática, tanto más imprevisibles serán las decisiones de los tribunales [...] Y cuanto menor sea el desarrollo dogmático, tanto más crece esa lotería, hasta llegar a una situación de aplicación caótica y sin rumbo de un Derecho pena [...] Donde están en juego pasiones humanas —y en qué proceso penal no ocurre así—, la fuente más turbia del conocimiento es un sentimiento jurídico no articulable conceptualmente."

e inclui os arts. 13- A e 13-B ao Código de Processo Penal, que conferem a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial. Também serão analisadas as decisões no RE 1.055.941, sob o regime da repercussão geral, no qual se discutia a possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte, obtidos pela Receita Federal no legítimo exercício de seu dever de fiscalizar, sem autorização prévia do Poder Judiciário, bem assim a decisão do RE 601.314, relatado pelo Min. Edson Fachin e julgado sob o rito da repercussão geral (tema 225).

Por fim, até em razão do objetivo geral deste trabalho estar relacionado à identificação de elementos que permitam superar um problema ainda em aberto na doutrina e na jurisprudência, também a dimensão normativa, na qual se faz uma análise valorativa das possibilidades abertas para defender aquela que se afigura como correta, será tratada na presente pesquisa.

2. REGULAÇÃO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

"Nós moldamos nossos edifícios e depois nossos edifícios nos moldam"
Winston Churchill

Em um discurso proferido em 1943, em meio às discussões sobre a reconstrução do edifício da Câmara dos Comuns em Londres, que havia sido destruído pelos bombardeios alemães na segunda guerra mundial, Winston Churchill defendeu a manutenção do formato tradicional do plenário, insistindo que o formato retangular da antiga Câmara havia sido responsável pelo bipartidarismo que era a essência da democracia britânica. Churchill, então, cunhou a frase que serve de epígrafe a este capítulo: "*we shape our buildings and afterwards our buildings shape us*."[41]

Anos depois, a frase seria reformulada por John Culkin, em um trabalho que ajudou a disseminar as ideias de Marshall McLuhan: "nós moldamos nossas ferramentas e em seguida nossas ferramentas nos moldam"[42]. A frase reflete bem as ideias de McLuhan, que, mesmo tendo falecido em 1980, anos antes da invenção da *World Wide Web* por Tim Berners-Lee, previu a existência da internet e a formação de uma aldeia global, afirmando que as ferramentas eletrônicas iriam provocar alterações na sociedade tão ou mais profundas do que a invenção da imprensa por Gutemberg[43].

A ideia de tecnologia evoca a utilização de técnicas modernas e complexas. Tecnologia, entretanto, não está necessariamente ligada à ciência de ponta e ao desenvolvimento de máquinas e aparelhos sofisticados, mas pode ser entendida como o conjunto de conhecimentos científicos ou práticos para a solução de problemas, mediante o uso de técnicas, máquinas e ferramentas (materiais ou não) para esta finalidade. Para utilizar uma definição que remonta a um artigo clássico do sociólogo Read Bain[44], tecnologia inclui toda e qualquer ferramenta, máquina, utensílio, arma, instrumento, mobiliário, vestuário, dispositivos de comunicação e transporte, bem como as habilidades pelas quais eles são

[41] PARLAMENTO DO REINO UNIDO. **Churchill and the Commons Chamber. disponível** em https://www.parliament.uk/about/living-heritage/building/palace/architecture/palacestructure/churchill/

[42] MCLUHAN GALAXY. **A Schoolman's Guide to Marshall McLuhan by John Culkin, S.J., 1967.** disponível em: https://mcluhangalaxy.wordpress.com/2017/09/19/a-schoolmans-guide-to-marshall-mcluhan-by-john-culkin-s-j-1967/

[43] CF KEEN, Andrew. **The internet is not the answer.** New York**:** Grove Press, 2015, p. 10 e ss.

[44] BAIN, Read. **Technology and State Government**. American Sociological Review, vol. 2, no. 6, 1937, pp. 860–874. disponível em www.jstor.org/stable/2084365.

produzidos e utilizados, constituindo-se, nessa concepção ampla, "no mais importante fator na produção, integração e destruição de fenômenos culturais"[45].

Ainda segue muito difundida a crença na tecnologia como algo apto a, por si só, solucionar a maior parte dos problemas que afligem a humanidade. De fato, há uma certa vinculação mental entre o potencial impacto das novas tecnologias nas tarefas cotidianas e sua aplicação prática, fazendo com que a maioria das pessoas, inclusive muitos teóricos, acabem se deixando encantar pelo imenso potencial das novas tecnologias e percam um pouco da necessária visão crítica acerca de sua aplicação concreta à sociedade.

A internet fornece um bom exemplo dessa visão otimista acerca do desenvolvimento das tecnologias, como bem demonstra o discurso do então presidente do Banco Mundial, James Wolfensohn[46], que, em uma conferência proferida em julho de 2000, afirmou que

> As novas tecnologias de comunicação e a queda dos custos da computação estão diminuindo as distâncias e reduzindo as fronteiras e o tempo - e as vantagens de um maior conhecimento e de uma maior capacidade de aprendizagem se tornam ainda maiores.
> A aldeia mais remota tem a possibilidade de explorar um estoque global de conhecimento além do que se teria imaginado um século atrás, e de forma mais rápida e barata do que qualquer um imaginava que seria possível apenas há algumas décadas[47].

Entretanto, essa visão extremamente otimista sobre os efeitos das novas tecnologias frequentemente não encontra eco na realidade que observamos. Para ficarmos no exemplo das novas tecnologias de informação e comunicação, basta lembrar os potenciais efeitos perversos que uma estrutura de controle como a internet pode gerar sobre as dissidências políticas e ideológicas, especialmente em locais com menor margem de atuação democrática. Não é por outra razão que Lessig[48] ressalta que o ciberespaço, deixado livre de regulação, acabaria se tornando uma ferramenta perfeita de controle. Não necessariamente controle pelo governo ou por alguma mente maligna, mas ainda assim uma forma de controle que seria muito distante

---

[45] IDEM, IBIDEM. Tradução nossa. No original: "is the most important single factor in producing, integrating and destroying cultural phenomena"

[46] WOLFENSOHN, James D. **Development and international cooperation in the twenty-first century : the role of information technology in the context of a knowledge-based global economy (ECOSOC).** 2000. Disponível em http://documents.worldbank.org/curated/en/519081467994605225/Development-and-international-cooperation-in-the-twenty-first-century-the-role-of-information-technology-in-the-context-of-a-knowledge-based-global-economy-ECOSOC-by-James-D-Wolfensohn-President

[47] Tradução nossa. No original: New communications technologies and plummeting computing costs are shrinking distance and reducing borders and time - and the advantages of greater knowledge and superior ability to learn become even greater. The remotest village has the possibility of tapping a global store of knowledge beyond what one would have imagined a century ago, and more quickly and cheaply than anyone imagined possible only a few decades ago.

[48] LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0,** New York: Basic Books, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf, p. 4.

dos ideiais libertários que orientaram a criação da internet. Como afirma Siva Vaidhyanathan[49],

> Embora tenha parecido óbvio e fácil declarar a ascensão de uma "sociedade em rede" na qual os indivíduos poderiam se realinhar, ganhar poder e minar os métodos tradicionais de controle social e cultural, parece claro que a comunicação digital em rede não precisa servir a tais fins libertadores.
> Na verdade, as disputas entre forças extremas – anarquia informacional e oligarquia informacional – tornaram qualquer formulação simples da nova era criativa quase imediatamente arcaica.[50]

Na verdade, essa visão exageradamente otimista e acrítica das novas tecnologias está na raiz de uma forma de compreender a relação da sociedade com a tecnologia conhecida como determinismo tecnológico ou tecnodeterminismo.

2.1 TECNODETERMINISMO E AS LEIS DE KRANZBERG

É muito comum que as novas tecnologias com características disruptivas sejam vistas através de um olhar tecnodeterminista, no qual elas passam a assumir quase que uma feição messiânica, com os analistas se limitando a descrever as “maravilhas” das novas tecnologias.

Cria-se, assim, uma visão triunfalista, que muitas vezes passa ao largo dos problemas reais e concretos criados pela implementação da tecnologia. As análises da relação entre sociedade e tecnologia baseadas nessa perspectiva tecnodeterminista seguem uma lógica muito própria, como apontado por Wilson III[51]. Elas partem sempre da tecnologia, com a descrição de seus aspectos mais marcantes e de seus componentes, para depois assinalar sua evolução recente, de modo a deixar clara sua importância. Em seguida, uma vez estabelecida e realçada a importância, o aspecto disruptivo e inovador passa a ser o foco da análise, com as propriedades internas da tecnologia sendo apresentadas como capazes de moldar toda a sociedade ao redor, o que inclui tudo, desde aspectos relativos às atividades econômicas e ao mercado de trabalho até a ampliação e promoção das liberdades públicas.

---

[49] VAIDHYANATHAN, Siva. **Remote Control: The Rise of Electronic Cultural Policy**. The Annals of the American Academy of Political and Social Science. N. 597, 2005. Disponível em https://www.researchgate.net/publication/228232631_Remote_Control_The_Rise_of_Electronic_Cultural_Policy

[50] Tradução nossa. No original: “While once it seemed obvious and easy to declare the rise of a ”network society” in which individuals would realign themselves, empower themselves, and undermine traditional methods of social and cultural control, it seems clear that networked digital communication need not serve such liberating ends.”.

[51] WILSON III, Ernest. **The Information Revolution and Developing Countries**. Londres: Routledge, 2004.

Essa análise, entretanto, deixa de atentar para os problemas e riscos decorrentes de sua aplicação concreta, especialmente aqueles ligados não só aos efeitos diretos da aplicação das novas tecnologias como, por exemplo, o aumento inicial do desemprego em decorrência da automação de uma dada tarefa), mas também para os possíveis "efeitos colaterais" da utilização da nova tecnologia, como a ampliação da desigualdade em decorrência da falta de acesso.

A visão tecnodeterminista tem como pressuposto a ideia da tecnologia como algo neutro, esquecendo sua origem eminentemente social. Nesse sentido, são comuns afirmações como a feita pelo diretor Geral da Nasdaq Bwise, Claudinei Elias, de que a "tecnologia é agnóstica"[52], querendo significar que a tecnologia é unicamente uma ferramenta que, do ponto de vista político e social, seria neutra, podendo ser utilizada para uma enorme variedade de finalidades, todas dependentes da intenção daqueles que as utilizam. Ocorre, entretanto, que tanto a internet, como qualquer outra tecnologia, sempre se desenvolve dentro de uma dada ordem social e econômica.

O mais grave problema dessa perspectiva tecnocêntrica é provavelmente que ela ignora as origens sociais das tecnologias de informação e comunicação, sugerindo que elas tenham surgido no vácuo, deixando de enxergar os interesses específicos que as geraram. Essa abordagem faz com que seja muito difícil para os responsáveis pela definição das políticas públicas perceberem que o atingimento do pleno potencial de uma nova tecnologia está muito mais ligado à organização institucional do que às suas características técnicas de desempenho. O desenvolvimento, a disseminação e a utilização da tecnologia, entretanto, estão longe de serem fatores neutros e isentos de efeitos perversos, podendo em muitos casos até mesmo ter o efeito de criar novos problemas sociais ou agravar os anteriormente existentes. Nesse sentido, vale notar que o Relatório de Desenvolvimento Humano 2019 do PNUD[53] chama atenção para o fato de que

> tem surgido uma nova geração de graves desigualdades no desenvolvimento humano, ainda que muitas das que ficaram por resolver no século XX estejam em declínio. Sob o espectro da crise climática e das arrebatadoras mudanças tecnológicas, as desigualdades no desenvolvimento humano têm assumido novas formas no século XXI. As desigualdades ao nível das

[52] CF. MEDEIROS, Henrique. **Nunca as leis de Asimov estiveram tão presentes, diz especialista em direito digital.** Mobiletime, 3/10/18 21:52. disponível em https://www.mobiletime.com.br/noticias/03/10/2018/nunca-as-leis-de-asimov-estiveram-tao-presentes-diz-especialista-em-direito-digital/

[53] PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO . **Relatório de desenvolvimento humano 2019.** Deisponível em http://hdr.undp.org/sites/default/files/hdr_2019_overview_-_pt.pdf

> capacidades estão a evoluir de variadas maneiras. [...]. as desigualdades no domínio das capacidades avançadas estão a aumentar, o que reflete aspetos da vida que, provavelmente, se tornarão mais importantes no futuro, ao proporcionarem uma maior capacitação. As pessoas que, nos dias de hoje, se encontram adequadamente capacitadas parecem destinadas a avançar ainda mais amanhã.

Por isso, é preciso sempre ter em mente que a análise de qualquer tecnologia (e com maior razão aquelas ligadas à informação e comunicação) deve ser sempre feita a partir de uma perspectiva ampla, que não se limite à descrição dos aspectos técnicos e evolutivos e no potencial disruptivo de sua implantação, mas que esteja atenta às consequências sociais, políticas e econômicas que a ela são inerentes. A dizer, apesar de ser evidentemente importante a análise de uma nova tecnologia levar em conta os seus aspectos técnicos e funcionalidades, a análise não pode ser limitada a tais aspectos. É preciso ter sempre em mente a inter-relação entre tecnologia e sociedade.

A tecnologia permeia a sociedade e media as relações dos homens entre si e com a natureza. Como afirma Castells, "a tecnologia é a sociedade, e a sociedade não pode ser entendida ou representada sem suas ferramentas tecnológicas"[54]. Há uma inter-relação dialética entre a sociedade e a tecnologia, de modo que a organização social condiciona o surgimento, o desenvolvimento e a disseminação das tecnologias, inclusive favorecendo ou desestimulando a criatividade e o empreendedorismo, da mesma forma que as tecnologias acabam por condicionar novas formas e processos sociais.

Nesse ponto, é preciso ainda estar atento para o fato de que, se por um lado não se pode adotar uma postura que pense a tecnologia como algo neutro e fora das relações humanas, por outro lado tampouco é possível sustentar-se uma perspectiva determinística, que enxerga na tecnologia a causa e a razão última para todas as mudanças sociais.

Assim, muito embora seja certo que a configuração da organização social permite estimular ou sufocar o desenvolvimento de novas tecnologias, especialmente por intermédio da atuação do Estado, a relação entre sociedade e tecnologia é dialética, e não determinística, por isso que a tecnologia não determina a evolução histórica ou as transformações sociais, mas incorpora a capacidade de transformação das sociedades e os usos que, a partir da correlação de forças existentes, a sociedade decide conferir a seu potencial tecnológico. Por isso, tanto parece inadequado adotar-se uma posição segundo a qual a tecnologia é neutra

[54] CASTELLS, Manuel. **A Sociedade em Rede – a Era da Informação: economia, sociedade e cultura**. 14a Reimpressão. São Paulo: Paz e Terra, 2011 , p. 43

("agnóstica"), quanto afirmar-se que a tecnologia determina linearmente a evolução da sociedade.

Nesse sentido, tem toda razão o historiador Melvin Kranzberg, fundador da Sociedade para a História da Tecnologia nos Estados Unidos, que, ao tratar do papel da tecnologia no desenvolvimento da sociedade, afirmou que é até possível aceitar-se a ideia bastante difundida segundo a qual a tecnologia apenas abre uma porta, mas não obriga ninguém a entrar. Entretanto, como ele bem ressalta, uma porta aberta é sempre um convite, sendo importante notar que há alguém que decide quais portas devem ser abertas. Além disso, uma vez que a pessoa decida aceitar o convite, sua jornada será guiada pelos contornos do corredor ou da câmara na qual ele entrou, sendo ainda igualmente importante saber se, tendo ingressado na porta, há alguma forma de voltar atrás[55].

Kranzberg afirma que, apesar de os historiadores ainda não terem chegado a uma resposta para a questão do determinismo tecnológico, os anos de imersão no estudo do desenvolvimento tecnológico e suas relações com as mudanças sociais lhe permitiram formular uma série de truísmos que sumarizam os consensos existentes acerca da relação entre a tecnologia e a sociedade, e que passaram a ser conhecidos como leis de Kranzberg e que, de um modo geral, podem servir de guia para a correta compreensão da relação entre a sociedade e a tecnologia:

1. **A tecnologia não é boa nem má; tampouco é neutra**. O desenvolvimento da tecnologia se dá dentro de um determinado ambiente social e suas consequências geralmente têm um alcance muito maior do que aquele inicialmente imaginado, por isso que uma mesma tecnologia pode ter resultados diferentes dependendo do contexto e das circunstâncias em que ela é introduzida;
2. **A invenção é a mãe da necessidade**. Todas as inovações implicam a necessidade de outros avanços técnicos para serem plenamente operacionais;
3. **A tecnologia vem sempre em pacotes, grandes e pequenos.** Os mecanismos complexos das tecnologias atuais normalmente envolvem vários processos e componentes;
4. **Apesar de a tecnologia constituir um elemento primordial em muitas questões públicas, há inúmeros fatores não técnicos que assumem**

[55] KRANZBERG, Melvin. **Technology and History: 'Kranzberg's Laws**. Technology and Culture, vol. 27, no. 3, 1986, pp. 544–560. Disponível em www.jstor.org/stable/3105385 .

precedência na tomada de decisões sobre a regulação das tecnologias. Há vários fatores essencialmente humanos na tomada de decisões sobre as tecnologias. Economia, religião, ideologia e várias outras razões socioculturais acabam exercendo um papel fundamental no desenvolvimento tecnológico, de modo que nem sempre a solução mais adequada tecnicamente triunfa sobre as forças políticas e sociais;

5. **Toda história é relevante, mas a história da tecnologia é a mais relevante.** Ignorar o elemento tecnológico no estudo da história pode fazer com que a disciplina perca relevância para a compreensão do presente e para a tomada de decisões acerca do futuro;
6. **A tecnologia é uma atividade essencialmente humana, assim como a história da tecnologia**. Por detrás de cada máquina há muitas faces. É necessária a atuação de engenheiros, operários, executivos, e um sem-número de outros profissionais para possibilitar o desenvolvimento e a implantação de uma nova tecnologia. Além disso, a função da tecnologia é essencialmente ser usada pelas pessoas - o que por vezes leva ao abuso ou à utilização incorreta.

Assentadas tais premissas, que servirão de guia para a presente investigação, cumpre notar, ainda, que vivemos tempos de intensas e radicais mudanças provocadas pelas novas tecnologias, cujos impactos são amplamente sentidos em nossa organização social. Esse fator certamente cria várias dificuldades para os analistas, dado que a análise de mudanças significativas que sejam contemporâneas aos analistas é muito difícil. Como bem salientou Sassia Sasken[56], frequentemente eles não terão o vocabulário, as categorias e as imagens mentais necessárias para capturar a mudança e isso é especialmente verdadeiro quando a aceleração da evolução tecnológica fez com que a sucessão de tecnologias disruptivas passasse a se dar em uma velocidade vertiginosa e inédita na história da humanidade.

De fato, entre o desenvolvimento da agricultura no crescente fértil e a invenção da roda houve um período de quatro mil anos. Entre a invenção da catapulta e a do canhão, houve um espaço de dois mil anos e entre a invenção do papel e a da imprensa por tipos móveis passaram-se mil anos. Entretanto, em um espaço de menos de um século, tivemos não só a invenção, mas também a massificação do uso de tecnologias como a dos automóveis a combustível, dos aviões, dos telefones, dos computadores, da internet, do *big data* e agora

[56] SASKEN, Sassia. **Losing Control?: Sovereignty in an Age of Globalization.** New York: Columbia University Press, 1996. Disponível em https://www.researchgate.net/publication/30529999

caminhamos a passos largos para a ampla difusão da inteligência artificial, da internet das coisas e da realidade aumentada, só para citar algumas das mais promissoras.

O primeiro computador digital eletrônico foi o ENIAC (acrônimo para *Electronic Numerical Integrator and Computer*), criado em 1949. Ele pesava cerca de 30 toneladas, ocupava toda uma sala de 10 x 15m e precisava de um ar condicionado de 10 toneladas para mantê-lo resfriado, tendo custado cerca de US$500.000,00. Com a invenção dos microprocessadores, no início dos anos 1970, desencadeou-se um processo tão rápido na evolução da computação que atualmente um pequeno microchip menor do que uma unha armazena uma quantidade de informação equivalente a 450,000 válvulas e é utilizado em um computador cujo custo é de menos de US$ 100,00[57].

Mas não foi somente o espantoso aumento na capacidade de processamento o responsável pelo imenso impacto da computação em nossas vidas. A ligação de computadores em rede teve um papel fundamental na construção do mundo digital em que atualmente vivemos, como será a seguir demonstrado.

2.2 A INTERNET E A SOCIEDADE DA INFORMAÇÃO

Entre as décadas de 1960 e 1980, os computadores, que haviam sido inicialmente criados como máquinas isoladas capazes de realizar operações lógicas e cálculos em frações de segundos, passaram a ser vistos como um meio de comunicação que permite que a informação seja quase instantaneamente compartilhada para qualquer localidade no mundo.

No início da era dos computadores, quando eles ainda eram máquinas gigantescas e extremamente caras, praticamente a única forma de se compartilhar informações entre eles era mediante a utilização de algum meio físico que permitisse a gravação da informação do computador de origem e que pudesse ser transportado até o local onde ficava o computador de destino. Apesar de os primeiros modems terem surgido no final da década de 1950, o ajuste de sua conexão à rede telefônica era caro, muito difícil e a conexão era bem instável. Como afirma Janet Abbate[58], um cientista que precisasse usar um computador que estivesse em um local distante certamente acharia mais fácil pegar um avião e ir pessoalmente até a localidade em que o computador se encontrava.

[57] KRANZBERG, Melvin. **Software for human hardware?** in ZUNDE, Pranas e Hocking, Dan. **Empirical foundations of information and software science.** New York.: Plenum Press, 1990. disponível em https://doi.org/10.1007/978-1-4684-5862-6_1

[58] ABBATE, Janet. **Inventing the internet.** Cambridge: The MIT Press, 2000.

A internet desenvolveu e popularizou a tecnologia de redes, colocando os computadores no centro das tecnologias de comunicação. Entre 1960 e 1990, a internet deixou de ser um experimento conectando uma dúzia de localidades nos Estados Unidos e se tornou uma rede que conecta todo o globo.

A cada dia a internet se firma mais como uma infraestrutura essencial para uma enorme gama de serviços e setores sociais, a ponto de ter se tornado lugar comum falar-se na existência de uma sociedade da informação[59]. Para Manuel Castells, vivemos uma nova era, em que o padrão de relação entre a natureza e a cultura alcançou um estágio tal que a convergência da evolução histórica e a transformação tecnológica engendraram um modelo genuinamente cultural de interação e organização social, no qual a informação representa o principal ingrediente de nossa organização cultural[60]. O desenvolvimento de uma sociedade global da informação diminuiu consideravelmente os custos da informação e de transação, criando o que muitos autores chamam de "sociedade da informação", definida por Marsden como aquela que

> atualmente está sendo construída, onde o baixo custo da informação e as tecnologias de armazenamento e transmissão passaram a ser de uso geral. Esta generalização da informação e do uso de dados é acompanhada por inovações organizacionais, comerciais, sociais e legais que irão modificar profundamente a vida tanto no mundo do trabalho quanto na sociedade em geral[61]

Ainda é cedo para saber se o período que vivemos poder ser classificado como uma nova era histórica, a da sociedade global da informação, marcada pela vida digital e pela construção de um novo local de interações sociais, diferente do espaço físico, o ciberespaço[62]. Inexiste consenso entre os autores que estudam a sociedade e as novas tecnologias sobre estarmos ou não em uma nova era. Entretanto, por mais diversas que sejam suas visões acerca

---

[59] Essa referência tornou-se de tal forma difundida que a expressão guarda pouca precisão analítica, por vezes referindo-se a realidades diversas. Para maiores discussões quanto ao sentido da expressão, ver WERTHEIN, Jorge. **A sociedade da informação e seus desafios,** disponível em http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf.

[60] CASTELLS, Manuel. **A sociedade em rede. Volume I**. P. 573

[61] MARSDEN, Christopher. **Information and communications technologies, globalization and regulation.** in MARSDEN, Christopher (org). **Regulating the Global Information Society.** Londres: Routledge, 2000.p.1. (tradução nossa).

[62] "Ciberespaço" é aqui entendido como algo distinto da internet, já que esta é apenas a base física da rede mundial de computadores, o meio sobre o qual aquele é construído. A expressão "ciberespaço", refere-se a uma experiência mais profunda, que envolve a utilização das estruturas de conexão de rede de tal forma a criar um espaço de comunicação no qual o usuário imerge. Vale notar, ainda, que a referência a um mundo "virtual" não se contrapõe ao mundo "real", uma vez que, o virtual, mesmo sendo fruto da engenhosidade humana, compõe também uma parte da realidade. Sobre o tema, ver LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0**, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf. p. 9 e SS.

das mudanças atuais, todos os autores concordam em um ponto: o reconhecimento do caráter especial da informação e de sua importância para o mundo contemporâneo[63].

As tecnologias digitais e as conexões em rede se tornaram tão onipresentes que hoje é quase impossível imaginar o funcionamento de nossa sociedade sem a internet. Para onde quer que se olhe, os impactos do uso das novas tecnologias de comunicação e informação, em especial da internet, são facilmente perceptíveis. Novos modelos de negócios são criados, trazendo consigo novas formas de produção, de troca e de consumo; no mercado de trabalho, diminuem os postos na indústria e crescem postos na prestação de serviços, especialmente na área informacional. Os novos meios digitais de comunicação em massa, como as redes sociais, blogs e canais de vídeos, cada vez mais se tornam referências culturais centrais, ocupando lugar que anteriormente foi dos meios tradicionais de comunicação, como jornais impressos, rádio e televisão. Novas redes são estabelecidas de modo a permitir contatos e interações imediatas, independentemente das distâncias geográficas[64]. Como afirmam Vint Cerf, Barry Leiner e David Clark, cientistas responsáveis pela criação da internet[65],

> A invenção do telégrafo, do telefone, do rádio e do computador criaram as condições para esta integração de capacidades sem precedentes. A internet é a um só tempo uma ferramenta com capacidade de transmissão mundial, um mecanismo para a disseminação de informação, e um meio para a colaboração e interação entre indivíduos e seus computadores sem levar em conta sua localização geográfica[66].

Por isso, compreender a sociedade atual passa necessariamente pela compreensão do funcionamento e da organização da internet, entendida, em termos gerais, como uma rede global que, por meio dos protocolos TCP/IP, conecta redes privadas, públicas, acadêmicas, comerciais e governamentais. Trata-se de uma rede, assim, que deixa de ter um caráter meramente local e passa a ter um escopo global.

Uma tal definição da internet torna necessário alguns esclarecimentos adicionais. Em primeiro lugar, cumpre notar que, apesar de comumente serem utilizados como sinônimos, os termos "internet" e "World Wide Web" (ou simplesmente "web") não são sinônimos. A

---

[63] WEBSTER, Frank. **Theories of information society**, 2014. p. 20

[64] Os exemplos aqui apontados correspondem às definições utilizadas por Frank Webster para categorizar as diversas concepções sobre a sociedade da informação (tecnológica, econômica, ocupacional, espacial e cultural), que são por ele analisadas sob uma perspectiva crítica no capítulo 2 de seu **Theories of information society**, 2014. PP. 10 – 23.

[65] LEINER, Barry M., CERF, Vinton G. CLARK, David D. et alli. **A brief history of internet.** Internet Society, 1997. Disponível em https://www.internetsociety.org/resources/doc/2017/brief-history-internet/

[66] Tradução nossa. No original: The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location

internet é uma rede global de conexão de computadores criada a partir de um projeto do Departamento de Defesa dos Estados Unidos e que conecta computadores utilizando um determinado conjunto de protocolos de comunicação (cujo funcionamento e arquitetura serão posteriormente detalhados). A *World Wide Web* é unicamente um dos serviços que essa rede global proporciona, isto é, a hospedagem de páginas com conteúdos que podem ser acessados por navegadores.

A "web", portanto, é o conjunto de documentos interligados por *hyperlinks* (conexões que ligam um recurso da rede a outro) e URLs ("*uniform resource locator*", ou "localizador uniforme de recursos", endereço de rede no qual se encontra algum recurso a ser acessado, como um arquivo ou um dispositivo como impressora, scanner, etc)[67]. Já a internet é a rede que possibilita não só o funcionamento da web, mas também inúmeros outros serviços, como e-mail, *streaming* de áudio e vídeo, transferência de arquivos, acesso remoto de computadores, grupos de notícias, jogos *online*, etc.

Essa distinção evoca uma discussão que durante algum tempo gerou polêmica, mas que a cada dia mais se torna superada: saber se "internet" é um nome próprio (que, portanto, deveria ser grafado com "i" maiúsculo) ou se é um nome comum, devendo ser escrito com letra minúscula. Inicialmente, era dominante a posição que defendia ser um nome próprio ("a Internet", escrita com letra maiúscula), como forma de ressaltar o fato de que, dentre inúmeras redes possíveis, somente poderia ser chamada de "a" Internet aquela em que a conexão se baseia no protocolo TCP/IP, ao passo que as demais redes, que adotassem um padrão de interconexão diferente (inclusive as privadas), deveriam ser simplesmente denominadas de internet. Nesse sentido, Bob Wyman, especialista em tecnologia da Google, escreveu em seu blog, em 2008[68], que "Se você nunca escreve internet com letra maiúscula, você está simplesmente indicando que não entende a distinção técnica entre a Internet e uma internet".[69]

A popularização da internet, entretanto, levou ao progressivo abandono dessa tendência de se referir à internet como algo único e específico o suficiente para receber um nome próprio. Veja-se que em 1999 o jornalista Stephen Wilbers já advertia que a internet e a

---

[67] WORD WIDE WEB CONSORTIUM. HTML **4.01 Specification.** Disponível em https://www.w3.org/TR/html401/struct/links.html#h-12.1

[68] HERRING, Susan C. **Should You Be Capitalizing the Word 'Internet'?** Wired. outubro de 2015. Disponível em https://www.wired.com/2015/10/should-you-be-capitalizing-the-word-internet/

[69] Tradução nossa. No original: "If you never capitalize internet, you are simply indicating that you don't understand the technical distinction between the Internet and an internet."

web estavam mudando e que tais mudanças fariam com que em breve deixassem de ser vistas como únicas e extraordinárias. Para ele[70],

> a maioria das pessoas (que não sejam *techies*) sequer sabem da existência de outras internets que não a internet - essa distinção não é mais relevante no dia a dia. E, para muitos jovens que cresceram com tecnologia, a própria internet é uma coisa ordinária - somente um outro meio de comunicação, como o telefone, a televisão e o rádio[71].

De fato, refletindo essa "ordinarização" do uso da internet, em 2016 o Manual de Estilo da Associated Press e o Manual de Redação do The New York Times passaram a recomendar que não fosse grafado internet ou web com letras maiúsculas[72]. Atualmente, não faz muito sentido pretender continuar tratando a internet como algo extraordinário, já que ela se integrou de tal forma à vida de todas as pessoas que é até difícil imaginar o mundo sem essa rede de interconexão de computadores, sendo certo que também as redes privadas de computadores acabam de alguma forma se conectando à internet e utilizando, os mesmos protocolos de interligação, uma vez que os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa.

A internet, tal como a conhecemos hoje, pode ser entendida, em linhas gerais, como o sistema global de informações que, segundo a definição do constante da Resolução de 14 de outubro de 1995 do Federal Networking Council (FNC) (i) é mantido logicamente ligado por meio de um endereço global único baseado no protocolo de internet (IP) ou por suas extensões e adições; (ii) é capaz de dar suporte a comunicações usando o Transmission Control Protocol/Internet Protocol (TCP/IP) e suas subsequentes extensões ou outros protocolos compatíveis; e (iii) fornece, utiliza ou torna acessíveis, de forma pública ou privada, os serviços de comunicação na mais alta camada.[73]

---

[70] CF. HERRING, Susan C. **Should You Be Capitalizing the Word 'Internet'?** Wired. outubro de 2015. Disponível em https://www.wired.com/2015/10/should-you-be-capitalizing-the-word-internet/

[71] Tradução nossa. No original: " Indeed, most people (other than techies) are not aware of any internets other than the Internet—that distinction is no longer relevant in ordinary usage. And for many younger folks who have grown up with the technology, the internet itself is ordinary—just another communication medium, like the telephone, television, and radio."

[72] CORBETT, Philip B. **It's Official: The 'Internet' Is Over**. The New York Times, Junho de 2016. Disponível em https://www.nytimes.com/2016/06/02/insider/now-it-is-official-the-internet-is-over.html

[73] Tradução livre. No original: The Federal Networking Council (FNC) agrees that the following language reflects our definition of the term ``Internet. ``Internet refers to the global information system that - (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the

Assim, chega-se ao ponto fundamental para a compreensão da internet: o protocolo TCP/IP ou, em outras palavras, a arquitetura da internet.

2.3 A ARQUITETURA DA INTERNET

A arquitetura da internet foi pensada a partir de protocolos de comunicação entre máquinas que permitem a interconexão entre elas. O conjunto de protocolos que garante essa comunicação funciona a partir da utilização de um modelo de camadas, no qual cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior.

Assim, a informação a ser transportada é quebrada em pacotes que trafegam pelas diversas camadas. Cada pacote carrega em si informações de endereçamento, o que permite que eles sejam direcionados corretamente ao endereço de destino, onde são agrupados para formar a informação buscada pelo usuário. As camadas da internet são seus componentes funcionais, e consistem provavelmente na principal característica que garantiu a generatividade da rede. As camadas mais altas estão logicamente mais perto do usuário e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração. São seis as camadas da internet[74]:

1) A camada de conteúdo, constituída pelos símbolos, sons e imagens que são apresentados aos usuários;
2) A camada de aplicação, utilizada para o envio e recebimento de dados pelos programas que utilizam a internet, tais como o WWW, o HTTP, o SMTP, o POP3, o IMAP, o DNS, o PING, etc;
3) A camada de transporte, o TCP, onde a informação recebida da camada de aplicação é "quebrada' em pacotes menores que serão organizados e encaminhados à rede;

communications and related infrastructure described herein. Disponível em https://www.nitrd.gov/fnc/internet_res.pdf

[74] CF. SOLUM, Lawrence B. e CHUNG, Minn. **The Layers Principle: Internet Architecture and the Law**, Notre Dame Law Review, vol. 815, 2004. Disponível em http://scholarship.law.nd.edu/ndlr/vol79/iss3/1

4) A camada de protocolo da internet (IP), que lida com o fluxo de informação pela rede. Nesta camada, os arquivos empacotados na camada de transporte são recebidos e anexados ao IP da máquina que envia e recebe os dados;
5) A camada de link, que faz a interface entre a máquina do usuário e a camada física, executando o recebimento ou o envio de arquivos na web;
6) A camada física, consistente nas estruturas físicas utilizadas para a transmissão dos dados, como os fios de cobre, a fibra ótica, os satélites de comunicação, etc.

Vale notar que essa não é a única classificação possível das camadas da internet. Anos após o desenvolvimento do protocolo TCP/IP, a *International Organization for Standardization* (ISO) desenvolveu um modelo de referência próprio para a interconexão de redes de computadores, que ela batizou de OSI (*open-systems interconnection*). Esse modelo conta com sete camadas (física, de conexão de dados, de rede, de transporte, de sessão, de apresentação e de aplicação). Em seu livro Weaving the Web[75], Tim Berners-Lee, criador da *world wide web*, identifica quatro camadas (de transmissão, de computação, de software e de conteúdo), numa aparente simplificação do modelo de referência OSI (*open systems interconnection*)[76].

Embora o modelo OSI tenha despertado bastante atenção no mundo acadêmico, inclusive tendo sido inicialmente adotado pela IBM e pela HP (que afirmavam que o protocolo TCP/IP era "coisa de pesquisadores"), foi o protocolo TCP/IP que acabou sendo adotado pela rede de computadores do Departamento de Defesa dos Estados Unidos e que foi adotado pela comunidade da internet[77].

As camadas da internet são organizadas em uma hierarquia vertical segundo a qual a informação que será transmitida pela internet sai da camada de conteúdo, que é a de nível mais alto, e passa sucessivamente pelas camadas de aplicação, transporte, IP e interface, até chegarem, já divididas em pacotes, à camada física, que é o nível mais baixo. Somente aí é que os pacotes de informação passam a trafegar horizontalmente até chegarem à máquina de destino, onde seguirão o caminho reverso, subindo da camada física até chegar à camada de conteúdo.

---

[75] BERNERS-LEE, Tim. **Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor**, San Francisco: HarperCollins, 2000.

[76] MURRAY, Andrew. **The regulation of cyberspace, Control in the online environment.** 2007, p. 43.

[77] HAFNER, Katie e LYON, Matthew. **Where wizards stay up late (the origins of the internet).** New York: Touchstone, 1998. p. 162.

O protocolo de comunicação da internet possibilita a comunicação fim-a-fim, especificando como a informação deve ser dividida em pacotes, endereçada, transmitida, roteada e recebida.

Com exceção da camada mais baixa, a camada física, todas as demais camadas são constituídas por algoritmos ou *software*. Dessas, duas (a de transporte e a do protocolo de internet) são parte do protocolo de comunicações que, como visto, é elemento central da internet, razão pela qual muitas vezes a camada de protocolo é muitas vezes chamada de camada de rede, sendo conhecida como a "camada que define a internet"[78].

O protocolo TCP/IP cumpre um papel essencial para o funcionamento da internet, permitindo-lhe funcionar como uma "rede das redes", por isso que não é exagero afirmar que, sem esse protocolo, a internet, tal como a conhecemos, não seria possível.

Por isso, é importante compreender, ainda que de um modo superficial, o funcionamento do sistema. Em uma obra de cunho eminentemente jurídico, obviamente que não se pode pretender buscar um aprofundamento necessário em aspectos técnicos, que frequentemente parecem incompreensíveis para a maior parte dos operadores do Direito. Entretanto, uma breve incursão sobre a história da internet pode fornecer os subsídios necessários à compreensão adequada do que é e de como funciona o protocolo TCP/IP.

O protocolo TCP/IP é o conjunto de protocolos de comunicação entre computadores desenvolvidos 1969 pela *Advanced Research Projects Agency* (ARPA) do Departamento de Defesa dos Estados Unidos, como um recurso para um projeto experimental chamado de ARPANET[79]. Essa agência governamental foi criada no contexto da guerra fria entre os Estados Unidos e a União Soviética, como uma resposta ao lançamento, pelos soviéticos, do primeiro satélite artificial, o *Sputnik.* A ideia inicial era criar uma agência que pudesse concentrar esforços em pesquisa avançada e desenvolvimento tecnológico para garantir que os Estado Unidos não mais ficassem em desvantagem na corrida tecnológica.

No rastro das experiências exitosas anteriores de integração entre militares e universidades no desenvolvimento de projetos científicos (foi assim que surgiram na segunda guerra mundial a tecnologia dos radares, as armas nucleares e as grandes máquinas de cálculos, por exemplo), a agência conferia ampla liberdade de pesquisa para os cientistas e recebeu polposos recursos públicos. Entre 1959, ano do lançamento do Sputnik, e 1964, os gastos em pesquisa e desenvolvimento dos EUA saltaram de US$ 5 bilhões anuais para mais

[78] SOLUM, Lawrence B. e CHUNG, Minn. **The Layers Principle: Internet Achitecture and the Law**, Notre Dame Law Review, p. 817.

[79] LEINER, Barry M., CERF, Vinton G. CLARK, David D. et alli. **A brief history of internet.** Internet Society, 1997. Disponível em https://www.internetsociety.org/resources/doc/2017/brief-history-internet/

de US$ 13 bilhões anuais. Como afirmam Hafner e Lyon, a "Sputnik lançou uma era de ouro para a ciência e tecnologia militares"[80].

Um dos principais projetos desenvolvidos pela agência era a criação de uma rede que permitisse a conexão de computadores que estivessem fisicamente distantes, já que, como afirmado, fazer com que computadores diferentes pudessem operar em conjunto era um desafio quase insuperável àquela época.

É interessante notar que a ideia comumente disseminada de que a internet foi pensada pelo Departamento de Defesa dos EUA como uma forma de garantir o funcionamento de sua rede de comunicações mesmo diante do advento de uma hecatombe nuclear, não é totalmente verdadeira, aproximando-se muito mais de uma lenda urbana do que daquilo que efetivamente ocorreu, e provavelmente se deve ao fato de que Paul Baran, um engenheiro que trabalhava na Rand Corporation e desenvolvia a ideia de "quebrar" os dados em pacotes para serem transportados pela rede de telecomunicações, ter trabalhado com essa ideia para emplacar seu projeto junto à força aérea americana.

Na verdade, entretanto, o objetivo inicial para o estabelecimento de uma rede de computadores como um projeto especial da ARPA foi bem mais prosaico: reduzir os crescentes gastos com a instalação de computadores para os pesquisadores. Com efeito, dependendo do computador utilizado e do número de pessoas envolvidas na pesquisa, os valores de financiamento de pesquisas no IPTO (*Information Processing Techniques Office*), setor da ARPA responsável pelas pesquisas da rede de computadores, variavam de US $500.000 a US$3 milhões. A ideia principal que moveu a busca pela construção de uma rede de computadores, portanto, era reduzir os gastos, criando uma rede que permitisse aos cientistas compartilharem os recursos computacionais[81].

Os mainframes típicos dos anos 60/70 eram pensados como máquinas que somente se conectam a alguns poucos periféricos bem específicos, desenhados para a realização de tarefas previamente determinadas e para a qual a programação seguia um fluxo unidirecional. Todos os aparelhos conectados ao computador estavam constantemente preparados para receber os comandos e executá-los da forma determinada, sem possibilidade de apresentar qualquer resposta diferente. Os computadores, portanto, somente enviavam comandos para os leitores de cartão, as unidades de fita e terminais, sendo que todos os "diálogos" entre as máquinas partiam do computador para o periférico ao qual ele devia dar instruções. Receber

[80] HAFNER, Katie e LYON, Matthew. **Where wizards stay up late (the origins of the internet).** New York: Touchstone, 1998. p. 13.

[81] MURRAY, Andrew. **The regulation of cyberspace, Control in the online environment.** 2007, p. 60

instruções de um outro computador era algo simplesmente fora de cogitação. O primeiro desafio de se estabelecer uma rede de computadores, portanto, foi o de possibilitar que os computadores se reconhecessem e admitissem receber comandos de outras máquinas.

O primeiro protocolo de comunicação estabelecido foi o *Host-to-host*, desenhado para possibilitar que computadores diferentes pudessem reconhecer comandos enviados de um para o outro. Em linhas gerais, esse protocolo definia como um computador deveria tratar o pacote de informações enviado pelo outro que a ele se conectasse, permitindo a troca de pacotes entre eles.

Pouco tempo após o início das atividades da ARPANET, Bob Kahn e Vint Cerf buscavam meios de fazer com que a recém-nascida rede pudesse fazer a interconexão de computadores ligados a redes diferentes. A solução que eles desenvolveram foi a criação de *gateways*, isto é, computadores roteadores que ficariam entre essas diversas redes e que teriam a função de entregar as mensagens enviadas de uma rede para a outra. Isso, entretanto, teria que ser feito sem que os pacotes de mensagens que eram transportados pudessem ser alterados. Para isso, o protocolo de comunicação então utilizado (*host-to-host*) seria inadequado, pois ele otimizava a entrega de pacotes especificamente no ambiente para o qual ele havia sido planejado. Para conseguir tornar a interconexão efetiva, seria necessário o desenvolvimento de um protocolo de comunicação mais independente do ambiente da rede ou do conteúdo da mensagem.

Foi então que, com o objetivo de resolver esse problema de interconexão de redes diferentes, Vint Cerf e Bob Kahn criaram um novo protocolo de transmissão de pacotes nas redes de computadores, que foi divulgado em 1974 no artigo "A Protocol for Packet Network Intercommunication.". No artigo, eles propunham que as mensagens fossem encapsuladas em "datagramas", como cartas dentro de um envelope, e que fossem encaminhadas como pacotes fim-a-fim, de modo que o conteúdo das mensagens não fosse objeto de atenção pela rede. Também introduziram ideia dos *gateways*, que apenas fariam a leitura do "envelope". Esse protocolo de comunicação foi chamado de *transmission-control protocol,* ou TCP. A ideia geral era a de que, nesse novo protocolo de comunicação, a confiabilidade da transmissão, isto é, a verificação da correção e da integridade dos dados transmitidos, deixasse de ser tarefa da rede e passasse a ser desempenhada pelos *hosts* de destino[82]. Nas palavras de Vint Cerf,

[82] HAFNER, Katie e LYON, Matthew. **Where wizards stay up late (the origins of the internet).** New York: Touchstone, 1998. p. 148

> Nós focamos na confiabilidade fim-a-fim. Não confiamos em nada dentro daquelas redes. A única coisa que pedimos à rede é que pegue esse pedaço de bits e o leve pela rede. É tudo o que pedimos. Pegue este datagrama e faça o possível para entregá-lo[83].

A invenção do protocolo TCP foi crucial para a viabilização da internet, pois, ao concentrar as tarefas mais complicadas às pontas da rede, permitiu que as conexões entre computadores passassem a se dar de maneira simples e efetiva. Para Hafner e Lyon, "a mágica da internet é que seus computadores utilizam um protocolo de comunicações muito simples".

Em janeiro de 1983 a ARPANET oficializou o TCP/IP como protocolo a ser utilizado por aquela rede, criando, assim, as bases para a disseminação da internet como a conhecemos, que pôde se expandir para além dos limites dos centros de pesquisa nos quais foi desenvolvida. Um conceito central para o desenvolvimento da internet, diretamente ligado à escolha da arquitetura da rede, é que ela não foi desenhada para uma utilização específica, ou seja, quando se pensou na interconexão de computadores ligados a redes diferentes não se buscou otimizar a utilização para um determinado fim ou para um aplicativo específico, e é justamente essa característica que possibilitou o surgimento de diversos usos e aplicações não previstas anteriormente, inclusive a *World Wide Web.*

Vale notar que essa arquitetura da rede decorreu de uma escolha consciente de seus idealizadores, como fica claro ao se verificar que, à época da criação do TCP/IP, Bob Kahn já defendia a adoção de quatro regras fundamentais da rede[84]:

> 1- Cada rede distinta teria que ser autônoma e nenhuma mudança interna poderia ser exigida em qualquer rede para conectá-la à Internet;
>
> 2- As comunicações seriam feitas com base no melhor esforço. Se um pacote não chegasse ao destino final, em breve seria retransmitido da origem;
>
> 3- Caixas pretas seriam usadas para conectar as redes; mais tarde, eles seriam chamados de gateways e roteadores. Não haveria informações retidas pelos gateways sobre os fluxos individuais de pacotes que passam por eles, mantendo-os assim simples e evitando adaptação e recuperação complicadas de vários modos de falha;

---

[83] APUD HAFNER, Katie e LYON, Matthew. **Where wizards stay up late (the origins of the internet).** New York: Touchstone, 1998. p. 149. Tradução nossa. No original: "We focused on end-to-end reliability, [...]. Don't rely on anything inside those nets. The only thing that we ask the net to do is to take this chunk of bits and get it across the network. That's all we ask. Just take this datagram and do your best to deliver it."

[84] LEINER, Barry M., CERF, Vinton G. CLARK, David D. et alli. **A brief history of internet.** Internet Society, 1997. p. 6

4- Não haveria controle global no nível de operações;

Além de tais regras, Vint Cerf, Bob Kahn e os demais inventores da internet afirmam que havia algumas outras preocupações centrais e que acabaram redundando em opções de arquitetura que foram implementadas na rede[85]:

- Algoritmos devem evitar que pacotes perdidos desabilitem permanentemente as comunicações e possibilitem que sejam retransmitido com sucesso da fonte;
- Fornecimento de "*pipelining" host a host* para que vários pacotes possam ser encaminhados da origem ao destino, a critério dos hosts participantes, se as redes intermediárias o permitirem;
- Funções de gateway devem permitir o encaminhamento de pacotes de forma adequada. Isso incluiu a interpretação de cabeçalhos de IP para roteamento, manipulação de interfaces, quebrando pacotes em pedaços menores, se necessário, etc
- A necessidade de somas de verificação final, remontagem de pacotes de fragmentos e detecção de duplicatas, se houver.
- A necessidade de endereçamento global.
- Técnicas para controle de fluxo host-a-host.
- Interface com os vários sistemas operacionais

Verifica-se, assim, que a internet foi desenhada desde os seus primórdios para funcionar como uma rede *fim-a-fim*, na qual os pacotes de dados enviados por um terminal conectado a um dos pontos da rede deve chegar a outro terminal sem intervenções indevidas, de modo que, em regra, os intermediários *(gateways)* não interferem no conteúdo dos pacotes, estando a estrutura interna da rede voltada unicamente para encaminhar os pacotes de dados na direção do destinatário[86].

Os equipamentos utilizados para que a rede funcione executam funções relativamente simples, ligadas principalmente à transmissão dos dados, enquanto as funções mais complexas são desempenhadas pelas máquinas que se conectam à rede. Como afirma Marcel Leonardi, o *design* da rede constitui uma plataforma neutra, que não exerce nenhum tipo de controle sobre

[85] LEINER, Barry M., CERF, Vinton G. CLARK, David D. et alli. **A brief history of internet.** Internet Society, 1997. p.7

[86] CF. GETSCHKO, Demi. **As origens do marco civil da internet.** *In* LEITE, George Salomão e LEMOS. Ronaldo (coords). Marco civil da internet. São Paulo: Atlas, 2014, p. 13

o que está sendo transmitido, pelo que, "de modo sucinto e figurado, pode-se dizer que a internet não sabe para que fins está sendo usada"[87].

Essa marca de origem também se verifica naquela que provavelmente é a mais importante aplicação da internet, a WWW, criada por Tim Berners-Lee no CERN (E*uropean Centre for Nuclear Research*) como uma forma de tentar possibilitar uma melhor gestão da informação na internet, por meio da ligação de páginas através de *hyperlinks*, tornando mais fácil o compartilhamento de dados. A distinção entre a internet e a world wide web é elucidada pelo próprio Tim Berners-Lee[88],

> A Web é um espaço abstrato (imaginário) de informação. Na Net, você encontra computadores - na Web você encontra documentos, sons, vídeos, … informação. Na Net, as conexões são cabos entre os computadores; na Web, as conexões são links de hipertexto. A Web existe por causa de programas que fazem a comunicação de computadores na Net. A Web não poderia existir sem a Net. A Web tornou a Net útil porque as pessoas na verdade estão interessadas em informação (para não mencionar conhecimento e sabedoria!) e na verdade não querem ter que saber sobre computadores e cabos.[89]

Esse modelo aberto e descentralizado de funcionamento da rede favorece a inovação e a interoperabilidade, possibilitando novos usos e desenvolvimentos imprevistos, conferindo à internet a característica que Jonathan Zittrain, numa alusão ao sétimo estágio na teoria de desenvolvimento psicossocial de Erik Erikson, chama de generatividade[90], possibilitando que novos desenvolvedores, sem qualquer relação com os responsáveis pela rede ou com provedores de acesso, possam oferecer aos consumidores novos produtos e serviços.

Nesse ponto, tendo em conta que o objeto deste trabalho refere-se à utilização para efeitos penais de dados obtidos pela internet, tem-se que a correta compreensão do objeto da regulação deve ir um pouco mais além da internet e da web, para permitir uma análise também daqueles serviços que, sendo propiciados pela conexão dos computadores, permitiu a expansão da capacidade de obtenção e processamento de dados a um nível que certamente impactará profundamente as relações sociais em geral e a persecução penal em particular.

---

[87] LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2012. p. 153.

[88] WORLD WIDE WEB CONSORTIUM (W3C). **Frequently asked questions.** Disponível em https://www.w3.org/People/Berners-Lee/FAQ.html

[89] Tradução nossa. No original: "The Web is an abstract (imaginary) space of information. On the Net, you find computers -- on the Web, you find document, sounds, videos,.... information. On the Net, the connections are cables between computers; on the Web, connections are hypertext links. The Web exists because of programs which communicate between computers on the Net. The Web could not be without the Net. The Web made the net useful because people are really interested in information (not to mention knowledge and wisdom!) and don't really want to have know about computers and cables."

[90] CF. ZITTRAIN, Jonathan. **The future of the internet and how to stop it.** Yale University Press & Penguin UK, 2008. Disponível em http://nrs.harvard.edu/urn-3:HUL.InstRepos:4455262.

2.4. GENERATIVIDADE E TRATAMENTO DE DADOS COLHIDOS NA INTERNET

A interligação de computadores por todo o globo trouxe como efeito mais visível o aumento quantitativo das informações coletadas, transmitidas e processadas. A quantidade de informação disponível graças à internet é algo sem paralelo na história da humanidade. Em um único dia, o Google efetua 3,5 bilhões de pesquisas[91] e processa um volume de informações milhares de vezes maior do que todo o material impresso na Biblioteca do Congresso dos Estados Unidos. A quantidade de informação armazenada cresce a uma taxa quatro vezes maior do que a média da economia mundial, enquanto o crescimento da capacidade de processamento é nove vezes maior que o da economia[92].

Essa gigantesca quantidade de informação à disposição para processamento, que revolucionou a organização de nossa sociedade, somente foi possível pela utilização da internet,[93] que possibilitou o tráfego de informações em larga escala, a uma velocidade anteriormente inimaginável e de forma suficientemente simples e barata para permitir que a criatividade humana encontrasse campo fecundo para desenvolver suas possibilidades.

Entretanto, toda essa verdadeira revolução na forma como lidamos com a informação obviamente não pode ser reduzida a seu aspecto quantitativo, uma vez que também qualitativamente houve uma profunda alteração na forma de tratamento da informação em razão do advento da internet.

Pelo fato de estarmos imersos em uma sociedade onde a cada dia mais se torna natural termos acesso às facilidades da internet, muitas vezes é difícil até perceber todo o impacto que essa nova forma de comunicação gerou na forma como lidamos com a informação, por isso talvez um exemplo seja necessário para ilustrar os efeitos dessa diferenciação qualitativa: os registros de ações judiciais sempre foram públicos, até como decorrência do devido processo legal e da imparcialidade do Judiciário. O segredo de justiça é algo excepcional, reservado para situações limítrofes. Entretanto, a partir do momento em que os processos se tornaram eletrônicos e o tratamento de um imenso volume de informações processuais passou a poder ser feito de modo rápido e barato, criou-se uma situação paradoxal, onde uma garantia

---

[91] CF. https://www.internetlivestats.com/google-search-statistics/#trend

[92] MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth. **Big Data : como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**, 2013, p. 5

[93] CF. LESSIG, Lawrence. **The Future of Ideas: the Fate of the Commons in a Connected World,** New York: Random House: 2001. disponível em http://www.the-future-of-ideas.com/download/lessig_FOI.pdf

fundamental do estado do direito, a publicidade processual, passou a representar um risco concreto à privacidade e a outros direitos fundamentais.

Para configurar-se essa nova situação de risco à privacidade sequer é preciso chegar a extremos mais evidentes, como ocorreria na obtenção de informações que envolvam discussões sobre temas mais sensíveis, como casos criminais ou ações envolvendo questões de saúde.

Na verdade, basta imaginarmos os potenciais efeitos dessa agregação de dados relativos a situações mais corriqueiras, como ações relativas a relações de consumo, ações de responsabilidade civil ou reclamações trabalhistas e pensar na possibilidade de empresas financeiras estabelecerem a partir de tais informações o perfil de risco de seus potenciais consumidores para definir se aprovam ou não um empréstimo, ou ainda na criação de "cadastros" de reclamantes em ações trabalhistas, para vermos como o processamento maciço de informações pode transformar dados públicos e cuja divulgação pareça algo singelo e desimportantes em informações valiosas, que podem definir a vida de pessoas sem que elas sequer se deem conta disso.

Aliás, não foi por outra razão que a França recentemente proibiu a utilização de dados relacionados a juízes ou servidores do judiciário para "avaliar, analisar, comparar ou prever suas práticas profissionais, reais ou supostas"[94]. Segundo a reportagem, essa medida, que tipificou criminalmente a conduta de quem publica o resultado dessas análises, teria sido adotada em razão do receio da prática de empresas que usam inteligência artificial para, com base em dados públicos, analisar como os magistrados costumam decidir e se comportar em determinados assuntos para tentar prever o resultado de julgamentos.

A vigilância governamental é uma outra área em que se pode verificar de forma muito evidente as consequências dessa nova forma de coletar, transmitir e processar informações, que criam possibilidades inexistentes anteriormente.

Um bom exemplo é a forma como a Interpol passou a lidar com seu banco de dados de passaportes furtados e extraviados. Da base de dados da Interpol constam mais de 39 milhões de ocorrências, que são alimentadas por 166 países. Atualmente, graças aos recursos computacionais, é possível aos agentes de segurança nos aeroportos verificarem em uma fração de segundos se os documentos apresentados pelos passageiros estão na lista da interpol. Por isso que, como afirma Amitai Etzioni, a diferença entre a coleta e processamento

[94] RODAS, Sérgio. **França proíbe divulgação de estatísticas sobre decisões judiciais.** Conjur, 5 de junho de 2019. Disponível em https://www.conjur.com.br/2019-jun-05/franca-proibe-divulgacao-estatisticas-decisoes-judiciais

de informações no mundo digital e no mundo analógico "é muito maior do que a diferença entre o impacto de uma granada de mão e o de uma bomba nuclear"[95]

De qualquer forma, os dados disponibilizados pelos usuários e coletados na internet pelas empresas de tecnologia, seja pelo seu aspecto quantitativo, seja pelo aspecto qualitativo, assumem atualmente um papel essencial nas vidas das pessoas, o que atrai para este setor as atenções do estado regulador, que busca meios de intervir na atividade dos atores responsáveis pela prestação dos serviços digitais de forma a conformar sua atuação às finalidades definidas pelos agentes públicos, nomeadamente a tutela dos direitos dos cidadãos, por isso que um trabalho que se propõe a tratar da coleta de dados pela internet e sua utilização para efeitos penais não pode passar ao largo do *big data* e da inteligência artificial.

A ampla disseminação da internet e a enorme proliferação de serviços à disposição da população criou um ambiente digital extremamente complexo e prevalente. As facilidades proporcionadas pela computação em nuvem, pelo *big data* e pela inteligência artificial levaram ao desenvolvimento de uma enorme gama de serviços e comodidades digitais que, como contrapartida, requerem o compartilhamento de uma quantidade anteriormente inimaginável de dados sobre os usuários, possibilitando que os fornecedores de tais serviços tenham acesso a tantas e tão profundas informações acerca de seus usuários (que vão desde os gostos, preferências, orientações políticas, religiosas, morais, etc, até o completo histórico de localização e com quem a pessoa manteve proximidade física) que não é exagero afirmar que os detentores dos dados conhecem a intimidade dos usuários melhor do que suas próprias famílias.

De fato, a combinação de dados obtidos a partir de diversas fontes conectadas à internet, como buscadores de pesquisa, histórico de compras, histórico de buscas, postagens, curtidas e visualizações nas redes sociais, além do monitoramento de geolocalização pelo GPS dos celulares, fornecem uma descrição muito precisa não só dos hábitos, gostos e atividades do usuário, mas também de sua personalidade. Para Daniel Solove, estamos nos tornando uma sociedade de registros de dados, e nossos dados não são nossos, mas de terceiros[96] .

Nossos registros digitais revelam com quem falamos, onde estivemos, o que compramos, onde trabalhamos, como nos divertimos, com quem interagimos e fornecem uma

[95] ETZIONI, Amitai. **Privacy in a cyber age: policy and practice**. Studies in Cybercrime and Cybersecurity series. New York: Palgrave Macmillan, 2015. p. 20

[96] SOLOVE, Daniel J. **Digital Dossiers and the Dissipation of Fourth Amendment Privacy,** 75 South California Law. Review. 2002. Disponível em https://scholarship.law.gwu.edu/faculty_publications/943/

boa visão sobre nossas orientações políticas e religiosas, nossa situação financeira e aspirações. Trata-se do fenômeno conhecido como dataficação, que se refere à coleta de informações, inclusive de fontes que nunca haviam sido imaginadas como tal, para que elas sejam transformadas em dados que possam ser mensurados e analisados[97].

A dataficação não se confunde com a mera digitalização de dados. Basta se pensar no que ocorre com autos de processos judiciais digitalizados para que essa diferença fique evidente. O processo eletrônico é exemplo de dataficação, uma vez que todas as informações contidas nos autos do processo judicial, inclusive aquelas relativas ao conteúdo dos autos, ficam disponíveis para pesquisa, agrupamento, análise e quantificação, possibilitando que softwares de gestão de dados (plataformas de *business intelligence)* possam apresentar estatísticas detalhadas sobre o fluxo processual e sobre o conteúdo das decisões, por exemplo. Por outro lado, os processos que foram simplesmente digitalizados, isto é, que eram físicos e cujos autos foram escaneados e passados para uma plataforma eletrônica, não permitem toda essa análise dos conteúdos, sendo necessária a intervenção humana para traduzir a imagem "fotografada" da página dos autos físicos.

O processo de dataficação refere-se a uma nova forma de lidar com a informação, que foi potencializado pela tecnologia da internet e pela ampliação da capacidade de processamento dos modernos computadores. Atualmente, praticamente tudo é transformado em dado para ser mensurado. Até mesmo as relações pessoais, experiências e estados de humor dos usuários de redes sociais, atividades físicas, padrões de sono e batimentos cardíacos de usuários de aplicativos fitness e a localização das pessoas passaram a ser informações passíveis de serem coletadas e convertidas em dados mensuráveis e analisáveis. Como afirmam Mayer-Schonberger e Cukier[98],

> Estamos em meio a um grande projeto de infraestrutura que, de certo modo, rivaliza com os do passado, dos aquedutos romanos à Enciclopédia do Iluminismo. Somos incapazes de valorizar esse fato porque, ao contrário da água que flui pelos aquedutos, o produto de nosso trabalho é intangível. O projeto é a dataficação. Como aqueles outros avanços infraestruturais, ele gerará alterações fundamentais na sociedade.

[97] MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**. Rio de Janeiro : Elsevier, 2013, p. 51 e ss.

[98] MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**. Rio de Janeiro : Elsevier, 2013, p. 66.

Os dados coletados dos usuários de aplicativos conectados à internet, quando agrupados e tratados, criam um mosaico bastante revelador de nossa identidade que, quando acessível pelas autoridades encarregadas da persecução penal, se transformam em uma valiosa fonte de dados para investigações. Um ótimo exemplo disso são as informações relativas à localização dos usuários de celulares, coletadas continuamente por aplicativos como Google Maps, Waze, Facebook , etc. Para Andrea Peterson[99],

> Informações sobre onde seu telefone esteve podem parecer inócuas, mas pode ser surpreendentemente reveladoras. Os dados de localização podem identificar onde alguém dorme, onde trabalha, com quem toma uma cerveja, que profissionais médicos visita e a que reuniões políticas ou religiosas frequenta. E é quase impossível tornar esses dados anônimos porque, como afirmou Jeff Jonas, pesquisador da IBM e cientista-chefe do IBM Entity Analytics Group, as pessoas estão "vivendo em gaiolas", seguindo um cronograma padronizado em que trabalho e casa são marcadores fáceis de discernir.[100]

Essas informações são coletadas por meio de aplicativos e serviços prestados pela internet, mas o que torna possível a associação dessa enorme quantidade de dados é o *big data*, que não se confunde com a internet. A internet é o meio que possibilita a coleta e o compartilhamento de dados, mas o *big data* é mais do que a comunicação, pois está relacionado à possibilidade de aprender, a partir de uma grande massa de informações, coisas que não poderiam ser aprendidas se fossem utilizadas de fontes com menores quantidades de dados[101].

Há muitas definições diferentes sobre o que seja big data. Segundo o McKinsey Global Institute, *big data* refere-se a um conjunto de dados cujo tamanho vai além da habilidade típica que as ferramentas de banco de dados têm para capturar, armazenar, gerenciar e analisar. Trata-se de uma definição intencionalmente subjetiva e sem parâmetros fixos, de modo que, segundo a McKinsey, permanecerá válida mesmo quando a capacidade

---

[99] PETERSON, Andrea. **Your location history is like a fingerprint. And cops can get it without a warrant.** The Washington Post. 30 de julho de 2013. Disponível em https://www.washingtonpost.com/news/the-switch/wp/2013/07/31/your-location-history-is-like-a-fingerprint-and-cops-can-get-it-without-a-warrant/

[100] Tradução nossa do original: "information about where your phone has been might seem innocuous, but it can be surprisingly revealing. Location data can identify where someone sleeps, where they work, who they get a beer with, what medical professionals they visit and what political or religious gatherings they attend. And it's almost impossible to anonymize this data because, as Jeff Jonas, IBM fellow and chief scientist of the IBM Entity Analytics Group has argued, people are "living in habitrails," following a standardized schedule in which work and home markers are easy to discern.

[101] MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth.**The rise of big data. How it's chancing the way we think about the world.** Foreign affairs. may/jun 2013. disponível em : https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data

de armazenamento e processamento das máquinas aumentarem[102]. De acordo com o glossário da consultoria Gartner, *big data* são "ativos de informação de alto volume, alta velocidade e/ou alta variedade que exigem formas inovadoras e econômicas de processamento de informações que permitem uma visão aprimorada, tomada de decisões e automação de processos".[103]

Frequentemente as discussões sobre o *big data* vêm acompanhadas de referências de que sua principal nota característica seriam os chamados "3Vs": volume (quantidade de dados), velocidade (velocidade do processamento e de troca dos dados), e variedade (quantidade de fontes e tipos de dados).

Importante notar que, com a computação passando a mediar a maior parte das relações humanas, o vertiginoso aumento da quantidade de dados coletados e da capacidade de processamento que caracterizam o *big data* se tornou o componente fundamental de uma nova lógica de acumulação, o capitalismo informacional, que procura prever e modificar o comportamento humano como forma de gerar receitas e controle de mercado.[104] O *big data,* assim, não é uma tecnologia ou um efeito inevitável do desenvolvimento, mas é essencialmente uma construção social, um arranjo sócio-tecnológico que combina a tecnologia (o conjunto de software e hardware que possibilita a coleta e análise de uma vasta quantidade de informações em um curto período de tempo) com um processo pelo qual os algoritmos são utilizados para minerar as informações e encontrar padrões e correlações entre eles que permitam a realização de análise preditiva e sua utilização sob a forma de novas informações.[105]

Essa nova forma de lidar com a informação, a partir de fontes maciças de dados que cobrem grande parte ou até mesmo a totalidade do evento, representa uma mudança radical. Desde o século XIX nos acostumamos a trabalhar a partir de pequenas amostras para, a partir delas, fazermos inferências e deduções para compreendermos fenômenos de larga escala. Isso

---

[102] CF. MANIKA, James, CHUI, Michael, BROWN, Brad et alli. **Big data: the next frontier for innovation, competition, and produtivity.** McKinsey Global Institute, 2011. Disponível em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation#

[103] GARTNER. **Gartner Glossary. definition of big data.** disponível em: https://www.gartner.com/en/information-technology/glossary/big-data. Tradução nossa. No original: "Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation."

[104] ZUBOFF, Shoshana. ***Big other:* capitalismo de vigilância e perspectivas para uma civilização de informação.** in BRUNO, Fernanda et al. **Tecnopolíticas da vigilância. perspectivas da margem.** São Paulo: Boitempo, 2018. p. 18

[105] YEUNG, Karen. **Algorithmic regulation: A critical interrogation**. 2017. p. 9

era uma decorrência natural da limitação ao acesso às fontes de informação, que era próprio de uma era analógica.

Em um mundo digital, entretanto, é possível deixar de trabalhar com amostragens para trabalhar com informações que representam, senão a totalidade, pelo menos grande parte do fenômeno observado. Como consequência, há uma redução do rigor na análise individual de cada um dos dados, mas um aumento da precisão na análise global do fenômeno. Como afirmam Mayer-Schonberger e Cukier,

> em geral, o big data é confuso, varia em qualidade e está distribuído em incontáveis servidores pelo mundo. Com o big data, frequentemente nos satisfazemos com uma sensação aproximada de direção, sem a necessidade de um milimétrico conhecimento do fenômeno. Mas não abdicamos completamente da exatidão; apenas de nossa devoção a ela. o que perdemos em precisão microscópica ganhamos em visão macroscópica[106].

Uma outra consequência dessa nova forma de se tratar a informação, é que a busca pela causalidade deixa de ter tanta importância e se começa a admitir a que a tomada de decisões pode ser baseada na descoberta de padrões e correlações, ainda que inexista clareza acerca das relações de causa e efeito. Trata-se de uma profunda alteração na forma como compreendemos a realidade. Deixamos de nos basear na certeza da causalidade para adotarmos a probabilidade decorrente da relação estatística entre dois dados para fundamentar a tomada de decisões.

As correlações indicam a existência de uma ligação entre dois ou mais dados, permitindo a compreensão de sua prevalência no presente e ajudando a prever sua ocorrência no futuro. Assim, por exemplo, quando se verifica que há uma correlação forte entre os dados A e B, que geralmente ocorrem aos pares, torna-se possível afirmar que se no futuro for detectada a presença de A, B também estará presente. Não se trata propriamente de uma "previsão do futuro", mas da constatação de que há uma forte probabilidade de que o evento ocorra.

Evidentemente essa é uma simplificação bastante grosseira e superficial, já que no mundo real frequentemente a análise é feita a partir de inúmeras variáveis e com relações correlacionais multifacetadas. Em linhas gerais, entretanto, é esse tipo de análise, realizada a partir de quantidades expressivas de dados, que está na base dos algoritmos preditivos que são responsáveis por grande parte do sucesso da internet, possibilitando os resultados de

[106] MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**. Rio de Janeiro : Elsevier, 2013, p. 9.

buscadores como o google, as sugestões de vídeos no You Tube, de músicas no Spotify, de compras na Amazon ou de contatos no Facebook. Para Mayer-Schonberger e Cukier, "previsões com base em correlações estão na essência do *big data*. A análise de correlações hoje é usada com tanta frequência que às vezes somos incapazes de valorizar o caminho que ela construiu."[107].

O *big data* está diretamente associado à inteligência artificial e à utilização da matemática para processar uma enorme quantidade de dados para prever possibilidades, por isso que sua utilização está essencialmente ligada à realização de previsões.

De fato, o desenvolvimento e a evolução da inteligência artificial têm apresentado expressivos resultados, com aplicações nos campos econômico, científico e militar que fazem com que este seja um campo promissor para lucros de empresas privadas e vantagens geopolíticas para os estados nacionais, levando à criação de uma verdadeira "corrida" pelo desenvolvimento de tal tecnologia[108].

É cada vez mais comum ver máquinas passarem a exercer funções que até bem recentemente somente podiam ser realizadas por pessoas que tivessem conhecimento especializado, treinamento custoso ou autorização governamental. Desde funções triviais, como a tradução de textos ou o auxílio à digitação de palavras em smartphones, até funções altamente impactantes, como as operações financeiras transnacionais ou o reconhecimento facial de potenciais criminosos e terroristas, passando pelo auxílio na tomada de decisões nos campos do direito e da medicina, a IA vem se firmando como uma parte essencial de nosso modo de vida e está presente em inúmeras atividades. Não é por outra razão que, para Matthew Scherer,[109] já estamos vivendo a era das máquinas inteligentes.

Entretanto, apesar da força de que ainda gozam as ideias oriundas da ficção científica sobre inteligência artificial no imaginário popular, onde os computadores estariam sempre à espreita para exterminar a humanidade, no melhor estilo do robô Ultron do filme "vingadores: a era de Ultron" ou da rede Skynet do Exterminador do futuro, o fato é que, pelo menos diante do atual estágio de evolução da IA, a grande questão não é o domínio do mundo por máquinas inteligentes.

Na verdade, as aplicações de inteligência artificial destinam-se a usos bem mais corriqueiros, como, por exemplo, garantir que a máquina possa verificar se um dado e-mail é

---

[107] MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth. Op. Cit. p. 39.

[108] CAVE, Stephen e ÓHÉIGEARTAIGH, Seán S. **An AI Race for Strategic Advantage: Rhetoric and Risks**, 2018. Disponível em http://www.aies-conference.com/wp-content/papers/main/AIES_2018_paper_163.pdf.

[109] SCHERER, Matthew. **Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies**, 29 HARV. J. L. & TECH. 353,201

um *spam*, qual a melhor tradução para um texto ou se o automóvel autônomo deve acelerar, reduzir a velocidade ou parar ao chegar a um cruzamento. Tudo isso é feito a partir do processamento de uma enorme quantidade de dados, que possibilitam a realização das previsões.

Entretanto, se por um lado máquinas inteligentes com projetos autônomos de dominação mundial ainda são coisa de ficção, forçoso é reconhecer que a disseminação e a contínua evolução dessa tecnologia evidentemente acarreta uma série de riscos[110] que não podem ser negligenciados.

De fato, muito provavelmente os mais importantes riscos decorrentes da ampla utilização de inteligência artificial e big data para o processamento de dados coletados através da internet dizem respeito à dignidade da pessoa humana e à necessidade de se garantir um espaço individualizado e protegido onde cada pessoa possa livremente desenvolver sua personalidade da forma como melhor lhe aprouver, livre da vigilância, controle e interferência da(s) coletividade(s).

No campo da geopolítica, verifica-se uma escalada na busca pelo domínio da tecnologia da inteligência artificial pelas maiores potências globais. Nesse cenário, não espanta que grandes empresas invistam valores astronômicos no desenvolvimento da inteligência artificial[111], e governos de todo o mundo venham expressando muito claramente a importância que conferem ao seu desenvolvimento. Nesse sentido, o Conselho de Estado da China incluiu em seus objetivos, em 2017, um plano de desenvolvimento da IA "para garantir à China as vantagens do pioneirismo no desenvolvimento de IA" e o presidente da Rússia, Vladmir Putin, declarou que "quem quer que se torne o líder nesta esfera se tornará o governante do mundo".[112]

O simples fato de estar se disseminando uma retórica de corrida pelo desenvolvimento da IA em busca de vantagens estratégicas já representa, per si, um enorme risco, que, na visão

---

[110] Adotamos aqui a distinção entre riscos e perigos de Luhmann, para quem a nota diferenciadora estaria na ideia de causalidade. Riscos seriam os danos futuros decorrentes de uma decisão, ao passo que perigos seriam os danos futuros decorrentes de fatores externos. Assim, os riscos seriam os danos futuros decorrentes de uma decisão do indivíduo, ao passo que os perigos seriam os danos futuros decorrentes de causas externas. Cf. LUHMANN, Niklas. **El concepto de riesgo** *in* BERIAIN, Josetxo. (comp.) **Las consecuencias perversas de la modernidad. Modenidad, contingencia y riesgo** Barcelona: Anthropos, 1996, p. 144

[111] GRAEF, Aileen. **Elon Musk: We Are "Summoning a Demon" with Artificial Intelligence,** The Economist, UPI edição de outubro de 2014. Disponível em: http://www.upi.com/BusinessNews/2014/10/27/ElonMusk-We-are-summoning-a-demon-with-artificial-intelligence/4191414407652/

[112] CAVE, Stephen e ÓHÉIGEARTAIGH, Seán S. **An AI Race for Strategic Advantage: Rhetoric and Risks**, 2018. Disponível em http://www.aies-conference.com/wp-content/papers/main/AIES_2018_paper_163.pdf. p.2

de Cave e Óhéigeartaigh[113], podem ser divididos em três grandes grupos: os riscos relativos à retórica de uma competição pela superioridade na IA (que, mesmo que não reverta em uma corrida real, inviabiliza a cooperação); riscos de que efetivamente se instaure uma corrida pela inteligência artificial (com os consequentes riscos de que as precauções necessárias sejam deixadas de lado e de que conflitos entre os competidores – especialmente os estados nacionais – se tornem reais) e, por fim, o risco de que algum dos competidores se sagre vencedor numa eventual corrida pela IA (hipótese em que a concentração de poder nas mão do vencedor poderá ser um fator de grande desequilíbrio no conjunto de forças do mercado e da geopolítica internacional).

Por outro lado, analisando aspectos concretos e específicos da utilização da IA e dos riscos sociais e militares dessa tecnologia, um estudo patrocinado pelo instituto RAND, Think Tank norte-americano ligado às forças armadas daquele país, apresentam conclusões que, no mínimo, servem para elevar o nível de preocupação com a disseminação do uso da IA no que diz respeito à privacidade.

No estudo intitulado "The Risks of Artificial Intelligence to Security and the Future of Work", Osoba e Welser IV[114] analisaram os riscos da IA para a segurança e para o mercado de trabalho. Quanto à segurança, eles trabalham com a possibilidade de a aplicação da IA na vigilância (surveillance) e na cibersegurança abrir uma nova porta de entrada para pessoas e grupos mal intencionados, com o objetivo de disseminar desinformação, possibilitando a criação de um sistema que atuasse como uma espécie de "agente duplo", isso para não falar dos enormes riscos à privacidade decorrente da expansão das tecnologias de reconhecimento facial cumuladas com a possibilidade dos agentes estatais encarregados pela persecução penal obterem mandados de busca e apreensão ou medidas constritivas com base em dados obtidos pelas ferramentas de IA. No campo do trabalho, os autores afirmam que a IA trará impactos sociais significativos, pois a redução de demanda de trabalhos mecânicos e repetitivos certamente não se fará acompanhar pela correspondente capacitação das pessoas para as tarefas mais complexas.

O impacto das transformações sociais decorrentes das novas tecnologias de informação e comunicação, do *big data* e da inteligência artificial, atinge fortemente o Direito, já que os contornos e os limites da lei e da regulação face às novas tecnologias dificilmente podem ser muito bem estabelecidos. Assim, elementos que estão na base das

[113] CAVE, Stephen e ÓHÉIGEARTAIGH, Seán S. Op. Cit.

[114] OSOBA, Osonde A e WELSER IV, William. **The Risks of Artificial Intelligence to Security and the Future of Work**. 2017. Disponível em https://www.rand.org/pubs/perspectives/PE237.html

soluções tradicionalmente adotadas pelo Direito, especialmente do Direito Penal, como a importância do estabelecimento da relação de causalidade entre uma ação e sua consequência jurídica, perdem muito de seu sentido.

Essas tecnologias, tal como acontece em relação à internet e à web, também são frequentemente apresentadas sob um discurso tecnodeterminista que somente enxerga as vantagens. O *big data* e a IA são apresentados como solução mais eficiente para a tomada de decisões mais corretas e precisas. Segundo esse discurso, podemos sossegar e deixar que os algoritmos nos ajudem a preservar o meio ambiente, encontrem curas para doenças e tomem as melhores decisões em diversas áreas de nossas vidas, desde sobre que filme assistir no serviço de *streaming* até sobre quem deve ser contratado numa seleção de emprego. No limite, poderão até chegar a decidir quais as penas que deverão ser aplicadas aos criminosos (malgrado as experiências negativas registradas com os programas de auxílio a juízes criminais no estado de Wisconsin, nos EUA, que revelaram uma série de vieses fortemente racistas[115]).

O *big data*, entretanto, traz consigo alguns desafios que deverão ser devidamente tratados pelo estado de direito. Neil Richards e Jonathan King[116] apresentam três desses desafios sob a forma do que ele denomina de paradoxos do big data. O primeiro é o da *transparência.* Apesar de a IA lidar com informações privadas coletadas extensivamente, seu funcionamento quase sempre é completamente opaco, pois opera amparado por segredo comercial das empresas que o desenvolvem. O segundo paradoxo é o da *identidade*, já que ele busca identificar e rotular o indivíduo às custas da identidade individual e coletiva. Finalmente, o terceiro paradoxo é o do *poder*, já que, apesar de ser decantado o enorme poder do *big data* de transformar a sociedade, esse poder sempre está a serviço de empresas e governos, que já detêm poder em comparação com os indivíduos.

Há, portanto, um enorme desafio ao direito quando se trata da regulação dessas novas tecnologias, em particular quando se cuida da proteção do indivíduo ante o poder de grandes corporações ou do estado. Na era analógica, quando se discutia a delimitação do campo legítimo de atuação do poder público na persecução penal, buscando estabelecer-se o espaço juridicamente protegido do indivíduo, a principal questão a ser definida era se o Estado poderia coletar determinadas provas contra o indivíduo sem autorização judicial. Foi o que

---

[115] CF. MAYBIN, Simon. **Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA.** BBC News, 31 outubro de 2016. Disponível em https://www.bbc.com/portuguese/brasil-37677421

[116] RICHARDS, Neil. e KING, Jonathan. **Three paradoxes of big data.** Stanford Law Reviewonline Vol. 66:41. Disponível em https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_StanLRevOnline_41_RichardsKing.pdf

deu ensejo ao reconhecimento da necessidade de proteção do domicílio como um direito protegido pela cláusula da reserva de jurisdição e à necessidade de que a situação de flagrância que excepciona a necessidade de mandado judicial seja amparada em justa causa existente antes da entrada das forças policiais no domicílio[117].

Na atual realidade, entretanto, a ênfase da proteção à privacidade não pode mais recair sobre a coleta da informação, uma vez que no mais das vezes ela é disseminada com o consentimento do próprio titular do direito, que com um clique dá seu consentimento para a coleta, tratamento e compartilhamento de dados sensíveis, simplesmente se limitando a aceitar os termos de serviço de provedores, aplicativos e serviços fornecidos via web.

Todas essas questões reforçam a necessidade de que a regulação das novas tecnologias seja feita de modo a tentar sempre compatibilizar a liberdade para o desenvolvimento dos avanços necessários com a necessidade de se resguardar os direitos fundamentais individuais e coletivos.

A internet e o ambiente digital que sobre ela é construído, o ciberespaço, que inclui os aplicativos e serviços que coletam, armazenam e processam informações pessoais utilizando big data e inteligência artificial, constituem o principal desafio regulatório de nossa época, valendo notar que na regulação do ciberespaço, assim como na de todas as novas tecnologias, o momento em que se dá a regulação é uma variável de extrema importância, uma vez que a regulação das novas tecnologias encerra um paradoxo, conhecido como dilema de Collingridge[118], segundo o qual, quando as novas tecnologias ainda são incipientes e pouco difundidas, sua regulação e controle são fáceis, mas ainda não é possível antever quais riscos seu desenvolvimento poderá acarretar, de modo que a regulação ainda será desnecessária.

Por outro lado, quando as tecnologias já estão bastante estabelecidas e seus efeitos adversos já são conhecidos, a sua regulação se tornará difícil, cara e, por vezes, impraticável. Assim, tem-se que as possibilidades fáticas de regulação de uma nova tecnologia são inversamente proporcionais a seu grau de difusão e tempo de desenvolvimento, especialmente quando a regulação implicar a necessidade de alteração da arquitetura dos códigos em que se baseia a tecnologia.

---

[117] O Supremo Tribunal Federal definiu, em repercussão geral, que o ingresso forçado em residência sem mandado judicial apenas se revela legítimo – a qualquer hora do dia, inclusive durante o período noturno – quando amparado em fundadas razões, devidamente justificadas pelas circunstâncias do caso concreto, que indiquem estar ocorrendo, no interior da casa, situação de flagrante delito (RE n. 603.616/RO, Rel. Ministro Gilmar Mendes, DJe 8/10/2010).

[118] BAPTISTA ,Patrícia e KELLER, Clara Iglesias. **Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas.** RDA – Revista de Direito Administrativo, Rio de Janeiro, v. 273, p. 123-163, set./dez. 2016

Assim, a organização da internet em camadas e a forma de funcionamento do protocolo TCP/IP, bem como a forma de coleta, tratamento e utilização de dados pessoais, trazem profundos reflexos sobre as possibilidades regulatórias, já que, como afirma a célebre tese de Lawrence Lessig[119], a arquitetura dos sistemas (código dos algoritmos) é per si uma importante força regulatória, constituindo-se como a principal modalidade de regulação da internet.

As ideias acerca da regulação da internet desenvolvidas por Lessig assumem grande relevância na superação do paradigma tecnodeterminista, na medida em que, ao mesmo tempo em que afirma a extrema importância do papel desempenhado pela arquitetura na regulação da internet, ele rejeita a ideia de que a internet seja dotada de características intrínsecas e imutáveis decorrentes de sua natureza[120]. Ao contrário, a arquitetura da internet pode ser alterada, e a natureza plástica da tecnologia permite que ela seja alterada, seja para tutelar os direitos que entendemos importantes, seja para aumentar o controle, a vigilância e garantir maior dominação do mercado.

Assim, da mesma forma que a arquitetura de uma construção estimula e encoraja os seres humanos a atuarem de uma certa maneira quando em seu interior, também no ciberespaço a arquitetura impacta a ação humana, encorajando alguns comportamentos e desestimulando outros. A arquitetura da internet, portanto, foi a característica regulatória que permitiu a explosão de generatividade que vimos nas últimas décadas. Como afirmam Solum e Cung,[121] "a arquittura da internet é uma função do software (ou do código) e do hardware que constituem a internet. Software e hardware são os tijolos e a argamassa da Internet."

A compreensão dessa inter-relação entre a arquitetura da internet e seu funcionamento é essencial para que seja possível pensar na regulação da internet e das novas tecnologias, evitando-se cair na tentação de adotar discursos tecno-deterministas, para quem não haveria possibilidade de regulação, ou de abraçar soluções voluntaristas, que veem no Direito o poder de modificar amplamente a realidade sem levar em consideração os demais fatores que influenciam na regulação.

---

[119] LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0,** New York: Basic Books, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[120] LESSIG, Lawrence. Op. Cit**.** P. 32

[121] SOLUM, Lawrence B. e CHUNG, Minn. **The Layers Principle: Internet Achitecture and the Law**, Notre Dame Law Review, vol. 815, 2004. Disponível em http://scholarship.law.nd.edu/ndlr/vol79/iss3/1. tradução nossa. No original: "The architecture of the Internet is a function of the software (or code) and hardware that constitutes the Internet. Software and hardware are the bricks and mortar of the Internet."

Se o que buscamos é uma forma de domar as novas tecnologias, de modo a torná-las instrumento de promoção dos direitos fundamentais e de redução das desigualdades, é essencial conhecermos os limites e possibilidades da regulação e a forma como o Direito pode influenciar na construção de um ambiente que possibilite compatibilizar segurança jurídica com inovação.

Por isso, é necessário que façamos uma breve incursão sobre a regulação, de modo a estabelecer o conceito de regulação utilizado no presente trabalho, a partir da análise de teorias regulatórias de base, buscando compreender como se dá a regulação da internet a fim de que seja possível pensar em uma estratégia regulatória efetiva, que consiga compatibilizar o adequado o funcionamento do serviço, com a necessária abertura à inovação, com as finalidade públicas a serem definidas pelo regulador, inclusive aquelas relativas à proteção de direitos fundamentais.

2.5 REGULAÇÃO E GOVERNANÇA DA INTERNET

A enorme popularidade de produtos e serviços prestados através da rede mundial de computadores transformou empresas como Google, Microsoft, Apple e Facebook em gigantes transnacionais que por vezes parecem estar fora do alcance das normas editadas pelos estados nacionais, fazendo com que a efetiva regulação da atuação de tais corporações se torne um imenso desafio, não só em razão da existência de dificuldades jurídicas, mas também em razão da existência de questões técnicas que nem sempre são bem compreendidas pelos operadores do direito que desempenham o papel de agentes de regulação.

A arquitetura da internet torna muito difícil a implementação de normas de controle, o que, se por um lado constitui uma inegável vantagem do ponto de vista da possibilidade da evolução tecnológica e da tutela e proteção dos direitos à liberdade de expressão contra possíveis tentativas de censura, por outro lado torna a internet um campo profícuo para a prática de ilícitos.

Nesse ponto, vale ressaltar que, no presente trabalho, tomamos como ponto de partida a tese seminal de Lessig, segundo a qual a arquitetura da internet deve ser entendida como uma força regulatória. Os códigos seriam elementos regulatórios de extrema importância e atuariam juntamente com o Direito, as normas sociais e o mercado na regulação da internet. Em sua obra *Code and other laws of cyberspace*, Lessig defende que o ciberespaço requer

uma nova compreensão sobre o funcionamento da regulação, que deve ir além das leis e normas para reconhecer o papel regulador do código. Para ele,[122]

> No mundo real, nós reconhecemos como o direito regula - através das constituições, leis e outras normas. No ciberespaço nós temos que compreender como um um "código" diferente regula - como o software e o hardware (i. e. o "código" do ciberespaço) que fazem o ciberespaço ser o que é regula o ciberespaço como ele é. Como William Mitchell coloca, o código é a "lei" do ciberespaço. "Lex informática," como Joel Reidenberg primeiro colocou, ou melhor, o "código é lei"[123]

A afirmação de que "*code is law*", entretanto, deve ser corretamente compreendida, pois não significa que efetivamente a arquitetura da internet ou os códigos que formam seus algoritmos devam ser entendidos como normas, isto é, como prescrições de dever ser, mas querem significar que a arquitetura da internet e do ciberespaço são forças que condicionam os comportamentos humanos, mas que são plenamente modificáveis pela ação humana.

De fato, no mundo real, a geografia ou as condições reais nas quais são desenvolvidas as atividades humanas representam dados sobre os quais os homens podem atuar, modificando-os, mas cuja existência não é decorrência da criação humana. Eles são condicionantes prévias, possuindo uma natureza inerente com a qual forçosamente o homem terá que lidar. No ciberespaço, porém, toda a arquitetura é produto da mente humana, inexistindo uma base prévia à qual a ação humana deva se conformar, por isso que o ciberespaço pode ser completamente moldado, inexistindo uma natureza imanente da internet ou das aplicações que a utilizam[124].

O argumento central de Lessig é o de que a possibilidade de regulação da internet depende do código que ela utiliza. Para ele, algumas formas de arquitetura do ciberespaço estão mais sujeitas à regulação do que outras, de modo que saber como a internet – no todo ou em parte – pode ser regulada vai depender da natureza do código utilizado. A arquitetura da internet, isto é, os códigos que lhe conformam, afetam diretamente quando e quais comportamentos da rede podem ser regulados.

---

[122] LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0,** New York: Basic Books, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf p. 6.

[123] Tradução nossa. No original: " In real space,we recognize how laws regulate - through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates - how the software and hardware (i .e ., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law." "Lex Informatica, " as Joel Reidenberg first put it, or better, "code is law ."

[124] LESSIG, Lawrence. Op. Cit. P. 24

Para Lawrence Lessig[125], do ponto de vista do regulador, a internet apresenta três *bugs* ou imperfeições: não há modos simples e seguros de saber a identidade do usuário (apenas é possível identificar o endereço IP da máquina); não é possível saber com precisão e certeza a localização do usuário, pois os endereços IP da máquina são lógicos, e não físicos; por fim, a terceira imperfeição regulatória diz respeito à inexistência de rótulos nos pacotes de informação acerca de seu conteúdo, o que impede que se saiba qual o uso que a informação transportada terá.

A tais "imperfeições" regulatórias, decorrente do *design* da rede, devem se somar ainda os obstáculos técnicos à regulação estatal decorrentes da utilização de uma determinada arquitetura de sistema ou código de programação que inviabilize o controle.

As consequências mais importantes a serem extraídas da tese de Lessig são a de que: a) os códigos são completamente criados por pessoas, que têm ampla liberdade para criá-los de qualquer forma, pois, ao contrário do que ocorre no mundo físico, no ciberespaço não há limites e obstáculos colocados previamente pela natureza; b) a elaboração dos códigos pode ser capturada por grupos ou entidades externas, inclusive os governos[126].

Dessa forma, fatores como o anonimato dos usuários, o acesso livre e irrestrito a fontes de informação em qualquer lugar do planeta ou o princípio de comunicação fim-a-fim, que garante a ausência de discriminação no tráfego da rede, que configuram elementos centrais da arquitetura original da internet, não devem ser vistos como elementos decorrentes da natureza da internet, dado que são resultado de opções políticas que não têm nenhuma garantia de permanência.

Na verdade, essa constatação reforça a conclusão de que o desenvolvimento da internet, assim como de qualquer outra tecnologia, sempre se dá dentro de uma dada ordem social e econômica, de modo que não se pode adotar uma visão tecno-determinista. Como afirma Sassia Sasken[127], as redes digitais estão incrustadas tanto nas características técnicas e padrões de hardware e software quanto na estrutura real da sociedade e nas dinâmicas de poder. Não existe uma economia puramente digital, tampouco existe uma corporação ou comunidade inteiramente virtual. O ciberespaço está incrustado no mundo real, na sociedade real, e reflete as relações sociais nele existentes.

---

[125] LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0,** New York: Basic Books, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf. p. 35-36.

[126] CF. MURRAY, Andrew. **Nodes and Gravity in virtual space.** 5 Legisprudence 195, 2011. P. 202.

[127] SASSEN, Saskia. **Towards a Sociology of Information Technology** - Current Sociology, Maio de 2002, Vol. 50(3): 365–388 disponível em http://www.saskiasassen.com/PDFs/publications/Towards-a-Sociology-of-Information-Technology.pdf

Assim, seguindo a tese de Lessig, constata-se que não raro o código (isto é, os algoritmos que controlam o funcionamento do ambiente digital) acabam por vezes fazendo com que a arquitetura do sistema se imponha como um elemento que condiciona ou até mesmo pode chegar a impedir a atuação do regulador.

O fato de que o protocolo de comunicação da internet seja inteiramente formado por códigos faz com que, pelo menos em tese, a sua "natureza" seja moldável e esteja sempre sujeita a alterações. Obviamente, tais alterações não podem (ou pelo menos não devem) ser feitas de forma voluntarista, eis que qualquer alteração em uma estrutura tão essencial quanto pervasiva, como é a internet, pode ter consequências extremamente drásticas em todo o mundo.

Um exemplo que serve bem para ilustrar esse risco é o da criação de *backdoors* em aplicativos da internet, isto é, permissões ocultas de acesso para entes governamentais, tal qual ocorreu no programa PRISM, ou a utilização de criptografia que admita uma chave de acesso ao conteúdo de mensagens trocadas entre os usuários, medidas amplamente defendidas por agentes públicos no debate da regulação da internet e dos aplicativos de comunicação como WhatsApp e Telegram.

Ainda que tecnicamente seja possível e relativamente simples a implementação de tais medidas, o fato é que, uma vez inserida uma vulnerabilidade no sistema de segurança das aplicações da nternet, é virtualmente impossível controlar quem de fato terá acesso a esta falha e quem poderá dela se valer para obrtenção de fins ilegais ou criminosos. Na verdade, ao se admitir a alteração do *design* dos algoritimos para possibilitar que órgãos governamentais possam ter acesso às comunicações dos usuários, também estremos abrindo uma larga janela de oportunidade para que criminosos e pessoas mal intecionadas também acessem esses dados, possibilitando desde a ocorrência de fraudes até a utilização de informações potencialmente constrangedoras para chantagear pessoas. Na melhor das hipóteses, se estará possibilitando toda sorte de abusos e excesso por parte de autoridades públicas.

Da mesma forma, a inserção de falhas intencionais na criptografia poderia ter efeitos gravíssimos na confiabilidade e segurança das transações comerciais, financeiras e até mesmo na necessária manutenção do sigilo das próprias atividades investigatórias do Estado.

Isto não obstante, o fato é que não se pode negar a extrema regulabilidade da internet, que, como criação humana, está em constante mutação, sendo impossível afirmar-se com certeza quais serão os caminhos que seu desenvolvimento futuro tomará. Como afirma Tim

Wu[128], ninguém pode afirmar com certeza se no futuro olharemos a fase da internet aberta e sem fronteiras como uma curiosidade histórica, tal como olhamos hoje para o comunismo, por exemplo. Entretanto, a transitoriedade de todos os sistemas nos permite concluir que pelo menos alguns desses elementos que caracterizam a internet atual como algo único e diverso das demais tecnologias de comunicação estão fadados a desaparecer a médio ou longo prazo.

O que será mantido e o que está fadado a desaparecer depende de como a sociedade vai lidar com a tecnologia, isto é, de quais serão os caminhos escolhidos para sua evolução.

A dizer, se não há dúvidas de que a ação econômica é incrustada nas relações sociais, também em relação ao desenvolvimento tecnológico as relações sociais subjacentes cumprem um papel de extrema importância, já que as tecnologias de informação e comunicação não se desenvolvem no vácuo, mas antes são produtos de homens concretos e se destinam a resolver problemas (inclusive econômicos) concretos, produzidos a partir da rede de relações sociais.

Ademais, a regulação da internet e das tecnologias digitais representa um enorme desafio ao modelo tradicional de estado de direito, fundado no modelo *command end control*, no qual há o estabelecimento, pelas autoridades constitucionalmente competentes, de regras jurídicas que devem ser respeitadas e obedecidas por todos dentro do espaço territorial sobre o qual o estado exerce sua soberania.

O caráter transnacional e fragmentado da internet, que tem uma estrutura de abrangência global, aliado ao fato de que os provedores de aplicações muitas vezes não possuem servidores de armazenamento de dados ou sequer possuem representação comercial nos países em que se encontram os usuários dos produtos ou serviços, criam um amplo espaço de conflito de normas no qual a legitimidade do exercício do poder estatal é muito questionável, levantando dúvidas não só quanto a qual ordenamento jurídico deve ser aplicado, mas também sobre como garantir efetividade às normas eventualmente aplicáveis. Para Frydman, Hennebel e Lewkowicz[129], a necessária conexão entre soberania estatal, território nacional e a lei se perde quando se trata de regular a internet, e o direito internacional não oferece respostas claras sobre qual é a jurisdição competente ou a lei aplicável aos litígios.

Ora, um dos mais evidentes exemplos de exercício de soberania estatal é a definição de condutas tipificadas como crime, uma vez que o instrumental do direito penal é a mais

---

[128] WU, Tim. **Is Internet Exceptionalism Dead? .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** P. 179 e ss.

[129] FRYDMAN, B., HENNEBEL., L. LEWKOWICZ, G.,**Public strategies for internet Co-Regulation in the United States, Europe and China.** *In* BROUSSEAU, E., MARZOUKI, M., e MËADEL, C. **Governance, Regulations and Powers on the the Internet.** Cambridge: Cambridge University Press, 2008. Disponível em HTTP://ssrn.com/abstract=1282826.

poderosa arma de que dispõem os estados nacionais para o controle de condutas em seu território ou mesmo relativa a bens jurídicos que o Estado, no exercício pleno de sua soberania, decide proteger independentemente de a lesão ou ameaça de lesão terem ocorrido dentro de suas fronteiras (no caso de extraterritorialidade da aplicação da lei penal). Entretanto, quando contextualizado na internet, especialmente diante da ampla proliferação da computação na nuvem, onde sequer é possível definir-se com precisão o local de armazenamento dos dados, o modelo tradicional de estado de direito, fundado no estabelecimento, pelas autoridades constitucionalmente competentes, de regras jurídicas que devem ser respeitadas e obedecidas por todos dentro do espaço territorial sobre o qual o estado exerce sua soberania passa a ser constantemente posto em xeque.

Essa inter-relação entre os aspectos jurídicos, políticos e técnicos, inerentes à regulabilidade da internet são extremamente importantes para a correta definição do papel que cabe ao Estado em um mundo digital, especialmente em matéria penal, onde a necessidade de estabelecer os limites para a atuação legítima do poder público, demarcando o campo possível do exercício da liberdade individual, que fundamenta a privacidade digital, apresenta-se como uma das mais urgentes tarefas da ciência do direito.

Com vistas a trilhar esse caminho é que buscaremos compreender os limites e possibilidade da regulação da internet, tendo presente a existência de uma inter-relação dialética entre as quatro forças regulatórias que atuam nas novas tecnologias: a lei, o mercado, as normas sociais e a arquitetura[130], a fim de possibilitar a identificação de parâmetros legítimos de intervenção estatal sobre a privacidade digital na esfera penal.

Para isso, entretanto, é necessário que se faça um esclarecimento prévio acerca do que será entendido como regulação, ante a multiplicidade de definições e teorias regulatórias, dado que, como afirmam Baldwin, Cave e Lodge[131], a regulação, tanto na academia quanto na prática, tem se mantido como uma espécie de "alvo móvel" durante as últimas décadas, já que o conceito de regulação vem evoluindo e aumentando, para incluir outras áreas que não o tradicional estudo de normas e regras estabelecidas para regular uma determinada atividade econômica. Por isso, até para evitar eventual imprecisão semântica que leve a mal entendidos, é imperioso que desde logo seja esclarecido qual o conceito de regulação a ser utilizado.

---

[130] MURRAY, Andrew. **Nodes and gravity in virtual space.** p. 212

[131] BALDWIN, Robert, CAVE, Martin Cave e LODGE, Martin. **Introduction: Regulation—the Field and the Developing Agenda.** in BALDWIN, Robert, CAVE, Martin Cave e LODGE, Martin (orgs.). **The Oxford Handbook of Regulation.** Oxford: Oxford University Press, 2010, p. 12

2.5.1 Regulação

Em um conto intitulado *Everything and nothing*, Jorge Luis Borges narra a busca de um jovem artista para superar a condição de ser "um ninguém", tentando simular a vida dos outros como ator, ou, como autor, imaginando heróis e outras fábulas trágicas. Como autor, ninguém foi tantos homens como aquele, que "pôde esgotar todas as aparências do ser". Borges finaliza o conto narrando que, no momento de sua morte, ao se encontrar com Deus, ele disse ao Criador: "Eu, que tantos homens fui em vão, quero ser um eu". A voz de Deus então lhe respondeu, em um torvelinho: "Eu tampouco o sou; sonhei o mundo como sonhaste tua obra, meu Shakespeare, e entre as formas de meu sonho está tu, que como eu és muitos e ninguém".

Em certa medida, a situação de Shakespeare no conto de Borges é bastante similar à do conceito de regulação, que vem sendo expandido para abarcar uma enorme gama de situações, correndo risco de, ao buscar ser tudo, tornar-se nada. A definição do conceito de regulação constitui matéria de notória dificuldade. Trata-se de conceito polimórfico, cuja delimitação e alcance variam de acordo com a teoria regulatória de base adotada. Em suas versões mais restritas, o conceito de regulação é centrado na tentativa estatal de influenciar os comportamentos socialmente relevantes que podem causar efeitos adversos. Já nas definições mais amplas, a regulação abrange todas as formas de controle social, intencionais ou não, originada do Estado ou de qualquer outra instituição social[132].

Em um artigo publicado em 2002, Julia Black[133] reuniu as definições mais comumente utilizadas em obras acadêmicas sobre regulação, separando-as em três grupos:

1) regulação como a promulgação de regras pelo governo, acompanhadas de mecanismos de fiscalização e implementação, normalmente a cargo de uma agência pública especializada;

2) regulação como qualquer meio de intervenção estatal direta na economia, qualquer que seja a forma assumida por tal intervenção; e,

3) regulação como todo mecanismo social de controle ou influência de condutas, quer sejam intencionais ou não. As duas primeiras noções de regulação são claramente centradas na atuação estatal, assumindo a regulação como sendo uma atividade eminentemente estatal.

---

[132] MORGAN, Bronwen e YEUNG, Karen. **An Introduction to Law and Regulation: Text and Materials.** Cambridge: Cambridge University Press, 2007. p. 4

[133] BLACK, Julia. **Critical Reflections on Regulation**, LSE Centre for the Analysis of Risk and Regulation Discussion Paper 4, 2002. Disponível em http://www.lse.ac.uk/accounting/CARR/pdf/DPs/Disspaper4.pdf

Já a última definição abre margem para uma concepção mais descentralizada, mas é tão ampla que acaba tornando impossível estabelecer quais os limites do que poderia ser considerado regulação.

Em sentido similar, Tony Prosser[134] se refere à existência de duas visões distintas da regulação, uma mais restrita, prevalente nos discursos políticos, e uma mais ampla, que cada dia mais ganha espaço nos debates acadêmicos.

A visão mais restrita de regulação a identifica com o modelo clássico de "comando e controle", uma forma de controle estatal baseado no estabelecimento de normas que são implementadas pela ameaça de sanções. Nesse modelo, a regulação seria o oposto do livre mercado, consistindo em um ônus aos atores econômicos que somente se justificaria para correção de falhas do mercado. Nesta concepção, a criação de regras pelos próprios agentes econômicos representaria uma alternativa desejável, que aliaria a busca pela eficiência econômica com o respeito à liberdade e à autonomia privada.

No campo do Direito, o fenômeno regulatório é comumente pensado por essa ótica mais restrita, centrada na atividade estatal regulada pelo Direito Administrativo, o que certamente se explica como uma decorrência do monopólio do Estado na produção das leis e na coerção estatal que garante seu cumprimento. Como afirmam Morgan e Yeung[135], sob uma perspectiva jurídica tradicional, a forma paradigmática da regulação é a edição de uma lei por um legislador soberano.

A visão mais ampla da regulação, por seu turno, expande a atividade regulatória, que deixa de gravitar exclusivamente na órbita do Estado (através dos órgãos da administração ou de agências reguladoras autônomas) e passa a incluir a autorregulação, a coregulação e até mesmo a regulação por organizações privadas. Além disso, o escopo da regulação deixa de ser apenas a correção de falhas de mercado e a busca pela eficiência econômica, e passa a incluir vários outros objetivos[136].

De acordo com esta concepção ampla, as normas privadas são consideradas como parte integrante da regulação, não havendo uma distinção rígida, para efeitos regulatórios, entre regras estabelecidas pelo Estado, pelos agentes econômicos, pelas forças sociais ou mesmo pela tecnologia[137].

---

[134] PROSSER, Tony. **Two visions of regulation.** Paper by Tony Prosser for 'Regulation in the Age of Crisis', University College. Dublin, 2010. Disponível em http://regulation.upf.edu/dublin-10-papers/1H1.pdf

[135] MORGAN, Bronwen e YEUNG, Karen. **An Introduction to Law and Regulation: Text and Materials.** Cambridge: Cambridge University Press, 2007. p. 4

[136] PROSSER, Tony. Op. Cit.

[137] CF. BLACK, Julia.. **Critical Reflections on Regulation**,

Não é objetivo do presente trabalho tentar estabelecer um conceito definitivo ou "correto" de regulação, o que seria inútil e até mesmo ingênuo, pois desconsideraria o fato de que, em grande medida, as divergências conceituais nesse campo decorrem de diferenças políticas e ideológicas ligadas à compreensão do papel a ser desempenhado pelo Estado, de modo que a opção por uma ou outra definição traduz quase sempre uma opção política.

Entretanto, a necessidade de clareza impõe que desde logo explicitemos a que estamos nos referindo quando falamos de regulação, indicando qual o sentido em que empregamos o termo.

Vale notar que uma forma de se evitar as controvérsias acerca da definição da atividade regulatória seria a adoção de uma perspectiva funcional, que, ao invés de tentar definir o escopo da regulação, parte da identificação das funções essenciais que estão presentes em toda atividade regulatória. Hood, Rothstein e Baldwin[138], em uma perspectiva que eles denominam de cibernética, afirmam que todo e qualquer sistema de controle pressupõe a existência de um mínimo de três componentes: a) a capacidade de definição de padrões que permitam a identificação de situações desejadas dentro do sistema a ser controlado; b) a capacidade de obtenção de informações ou monitoramento sobre o estado atual ou sobre as mudanças ocorridas no sistema; c) a capacidade de modificar comportamentos de modo a alterar o estado do sistema a ser controlado.

Na ausência de qualquer desses fatores, o sistema não estará sob controle, de modo que estas seriam as funções essenciais presentes em qualquer modalidade de regulação.

A adoção de um conceito meramente funcional de regulação, porém, não parece ser suficiente para afastar o risco de possíveis equívocos e incompreensões na comunicação.

De fato, basta perceber que a chamada "desregulação", medida constantemente defendida como sendo essencial para uma maior eficiência econômica, é algo que só faz sentido se adotarmos a visão mais restrita de regulação, dado que na realidade este termo refere-se à descentralização da regulação, com a definição de padrões e a fiscalização das normas passando a ser feita pelos próprios agentes privados a quem tais padrões são aplicados.

Ora, se numa perspectiva restrita de regulação a desconcentração de produção e fiscalização normativa pode ser chamada de *desregulação*, o mesmo não ocorre quando se adota uma visão mais ampla de regulação, na qual também as regras produzidas pelos entes

[138] HOOD, Christopher, ROTHSTEIN, Henry e BALDWIN, Robert.**The Government of Risk: Understanding Risk Regulation Regimes.** Oxford: Oxford University Press, 2001.

privados (autorregulação) é considerada como atividade regulatória. Quando se adota uma perspectiva ampla de regulação, portanto, desregulação somente poderia se referir à total ausência de definição de padrão de conduta a ser seguida, já que mesmo a definição de termos de conduta do usuário estabelecidos nos contratos de adesão ou a escolha de determinadas arquiteturas de algoritmo configurariam forças regulatórias.

Da mesma forma, afirmações como a de Giandomenico Majone[139], de que o Estado regulador contemporâneo não foi precedido por um regime de puro laissez faire, mas por outro Estado regulador, diferente apenas "na forma, escopo e/ou nível de regulação, assim, como na importância relativa das políticas regulatórias ante outras funções governamentais", somente fazem sentido a partir de uma visão ampla de regulação.

É certo que a definição de um conceito nunca é neutra, na medida em que ela traz embutida uma enorme gama de valores e pré-compreensões teóricas e práticas. Assim, é inegável que adotar a noção mais restrita de regulação reflete, de forma consciente ou não, uma opção política de defesa de um programa de redução da intervenção estatal, o que é especialmente verdadeiro quando se trata da regulação das novas tecnologias, como a internet.

A própria noção de desenvolvimento tecnológico evoca as ideias de mercado, empreendedorismo, inventividade e liberdade de ação, ao passo que regulação remete a governo, burocracia e limites ao desenvolvimento de novas ideias.

Na internet, a regulação é quase sempre identificada com uma tentativa de restrição, controle ou ingerência estatal, e, por isso, é vista com muita desconfiança pela comunidade que atua na internet, tanto pela preocupação com a restrição da liberdade para usuários e desenvolvedores, quanto pelo receio de que os reguladores não compreendam corretamente questões técnicas de funcionamento da internet e editem normas que acarretem perda de eficiência, de estabilidade ou de segurança.

Assim, não parece adequada a utilização, no âmbito da internet, de um conceito restrito de regulação, centrado na atividade estatal de controle através da edição de normas cuja obediência é imposta pela ameaça da aplicação de uma sanção.

De fato, a visão da regulação da internet a partir de um conceito de regulação centrado na atividade estatal de controle implica necessariamente a defesa de uma posição política que privilegia a autonomia privada e os modelos de negócios criados no ciberespaço, fazendo com que toda atividade estatal, qualquer que seja seu conteúdo, seja vista com desconfiança.

---

[139] MAJONE, Giandomenico. **The transformation of the regulatory State.** Osservatorio sull'Analisi de Impatto della regolazione. 2010. Disponível em www.osservatorioair.it

A essa posição inicial de desvantagem no campo ideológico soma-se o fato de que um conceito restritivo de regulação teria pouca capacidade de rendimento teórico quando se busca discutir o ciberespaço. Isso porque a maior parte da internet é autorregulada, sujeitando-se a normas editadas por entidades como o ICANN (*Internet Corporation for Assigned Names and Numbers*), o W3C (*World Wide Web Consortium*) e o IETF (*Internet Engineering Task Force*), com uma interferência mínima de entes estatais.

Por isso, em relação à internet, onde a possibilidade de criação de novas tecnologias ou de novas formas de utilização das tecnologias já existentes é a característica que lhe garantiu a generatividade que a levou a atingir o atual estágio de desenvolvimento, a noção restrita de regulação parece ser insuficiente para a compreensão da totalidade do fenômeno. Nesta seara, é mais adequada a utilização de uma concepção ampla de regulação, que não se restrinja aos esforços estatais para dirigir a economia através da elaboração de regras, sua aplicação por meio de sistemas de coação e outros instrumentos governamentais, mas que permita abertura suficiente para incluir também outras forças regulatórias importantes não diretamente ligadas à atividade estatal.

Assim, no presente estudo adotaremos o conceito descentralizado de Black, para quem

> Regulação é a tentativa focada e sustentada de alterar o comportamento dos outros, de acordo com padrões ou objetivos definidos, com a intenção de produzir um resultado ou resultados amplamente identificados, que pode envolver mecanismos de definição de padrões, de obtenção de informações e de modificação de comportamentos.[140]

A adoção desta concepção ampla de regulação, ao mesmo tempo em que amplia as possibilidades analíticas no campo do Direito, também representa um enorme desafio, pois coloca em xeque três ideias amplamente aceitas pela abordagem jurídica tradicional da regulação[141].

Em primeiro lugar, o Estado deixa de ser visto como *locus* primário de articulação dos objetivos coletivos de uma comunidade, na medida em que se reconhece a emergência de outros fóruns deliberativos não governamentais, tais como empresas, associações da sociedade civil e movimentos sociais. Em segundo lugar, também perde força a ideia de que o

---

[140] BLACK, Julia.. **Critical Reflections on Regulation**, p.20. tradução nossa. No original: "Regulation is the sustained and focused attempt to alter the behavior of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information gathering and behavior modifications"

[141] MORGAN, Bronwen e YEUNG, Karen. **An Introduction to Law and Regulation: Text and Materials.** Cambridge: Cambridge University Press, 2007.

Estado tem autoridade final na definição dos padrões e objetivos a serem perseguidos pela coletividade, com o gradativo aumento da importância das noções de governança. Finalmente, também perde força o modelo de "comando e controle" como meio por excelência de conformação de condutas, tanto em razão dos problemas relacionados à efetividade desse modelo, seja em razão do reconhecimento da possibilidade de formas alternativas de implementação de políticas públicas.

A utilização do conceito amplo de regulação também tem a vantagem de permitir visualizar mais claramente as relações entre o desenho institucional da regulação, as estratégias regulatórias utilizadas e os resultados da regulação, sendo certo que, como salienta Black[142] é um dado empírico já bem reconhecido que a regulação, ao produzir mudanças de comportamento, gera também resultados não pretendidos (embora não necessariamente adversos).

No que diz respeito às estratégias regulatórias da internet, é possível divisar a existência de três formas de regulação:

a) Regulação direta, que ocorre quando a um ente estatal é atribuída competência para estabelecer normas impositivas aos regulados, verificar seu cumprimento e impor sanções;

b) Co-regulação, quando o ente estatal delega aos regulados a responsabilidade pela manutenção e aplicação de um código de conduta por ele aprovado, mantendo supervisão das atividades dos regulados e assegurando a possibilidade de intervenção onde e quando necessário. Vale notar que, como afirmam Frydman, Hennebel e Lewkowicz[143], a co-regulação não é mero modelo "intermediário", mas um modelo próprio e diverso, com sua própria racionalidade, baseado no empoderamento dos atores para que um possa controlar o outro;

c) autorregulação, quando os regulados, no mais das vezes um grupo de indivíduos ou de empresas, exercem controle sobre o comportamento e sobre o ingresso de outros no grupo. A entrada no grupo é voluntária e as normas são implementadas pelo próprio grupo, através da criação de códigos de conduta, estabelecimento de padrões ou implementação de soluções tecnológicas, sendo que a responsabilidade pelo monitoramento do cumprimento das normas cabe ao grupo, e não a uma entidade externa[144].

---

[142] BLACK, Julia.. **Critical Reflections on Regulation**. p. 4

[143] FRYDMAN, B., HENNEBEL., L. LEWKOWICZ, G.,**Public strategies for internet Co-Regulation in the United States, Europe and China.** *In* BROUSSEAU, E., MARZOUKI, M., e MËADEL, C. **Governance, Regulations and Powers on the the Internet.** Cambridge: Cambridge University Press, 2008. Disponível em HTTP://ssrn.com/abstract=1282826.

[144] MARSDEN, Christopher. **Internet co-regulation: european Law, regulatory governance and legitimacy.** Cambridge: Cambridge University Press, 2011.

O uso de diferentes instrumentos e estratégias regulatórias pode retardar ou acelerar as mudanças tecnológicas, ou mesmo influenciá-la em determinado sentido, favorecendo um certo tipo de tecnologia em detrimento de outros. Por isso é que, como afirma Jonathan Weiner[145], a regulação deve ser entendida em si como uma forma de tecnologia - a tecnologia da governança.

2.5.2 Governança

O conceito de regulação aqui adotado tem íntima relação com o de governança, a ponto de Dubash e Morgan[146], em obra que tratava da ascensão do Estado regulatório no sul, terem cogitado substituir a menção a "Estado regulatório" por "governança regulatória", considerando que este último termo "reflete melhor nossa própria atenção a como as instituições reguladoras interagem com outras instituições na formação de padrões de governança"[147].

O termo 'governança' começou a ser utilizado na Ciência Política e na Economia para se referir a uma forma de exercício do poder que não se limitasse unicamente ao aspecto estatal da governabilidade, mas que fosse além, para englobar a sociedade como um todo, incluindo "padrões de articulação e cooperação entre atores sociais e políticos e arranjos institucionais que coordenam e regulam transações dentro e através das fronteiras do sistema econômico"[148].

No relatório *Governance and development*, o Banco Mundial[149] definiu governança como "a maneira como o poder é exercido na gestão dos recursos econômicos e sociais de um município para o desenvolvimento". Para o Grupo de Trabalho das Nações Unidas,[150]governança na internet é "o desenvolvimento e aplicação por governos, setor

---

[145] WIENER, Jonathan. **Precaution in a multirisk world.** Duke Law School Public Law and legal Working Paper, 2002. Disponível em: http://scholarship.law.duke.edu/faculty_scholarship/1113.

[146] DUBASH, Navroz & MORGAN, Bronwen. **Understanding the Rise of the Regulatory State in the Global South**. Regulation & Governance. Oxford: Oxford University Press, 2012. p. 2

[147] Tradução nossa. No original: "better reflects our own attention to how regulatory instituitions Interact with other institutions in shaping patterns of governance"

[148] GONÇALVES, Alcindo. **O CONCEITO DE GOVERNANÇA.** Anais do XIV Congresso do Conpedi. 2006. Disponível em http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/XIVCongresso/078.pdf.

[149] Tradução Nossa. No original: " the manner in which power is exercised in the management of a county's economic and social resources for development"

[150] VAN EETEN Michel e MUELLER, Milton. **Where is the governance in Internet governance?** New Media & Society, 2012. Disponível em https://www.researchgate.net/deref/http%3A%2F%2Fnms.sagepub.com%2Fcontent%2Fearly%2F2012%2F11%2F19%2F1461444812462850.

privado e sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomada de decisão e programas compartilhados que moldam a evolução e o uso da internet"[151].

Um ponto comum a todas as definições de governança é a noção de direcionamento e moldagem, mas de uma forma mais leve do que aquela tradicionalmente associada ao conceito de governo. É exatamente pela maior extensão horizontal e menor profundidade vertical que o conceito de governança ganhou espaço no campo das relações internacionais, já que denota relações menos baseadas em uma hierarquia central e mais inclusivas de diferentes atores sociais que atuam de forma interdependente.

Por isso é que, como afirma Milton Mueller[152], a governança na internet é o mais simples, direto e inclusivo rótulo para o contínuo conjunto de disputas e deliberações sobre como a internet é coordenada, gerenciada e moldada para refletir políticas. A definição de governança, assim, implica na adoção de um conceito relacional, ligado a processos compartilhados que envolvem governos, empresas e sociedade civil.

Uma vez fixado o sentido dos termos regulação e governança da internet, afastado o risco de incompreensões e equívocos decorrentes de imprecisões terminológicas, cabe agora verificar de que forma têm sido apresentados os argumentos na discussão acerca da regulabilidade da internet e da proteção à privacidade digital.

Nesse sentido, é importante aprofundar a discussão acerca de duas ideias muito difundidas no debate regulatório da internet e das novas tecnologias de informação e comunicação, mas que frequentemente não são postas de forma explícita, funcionando unicamente como ideias subjacentes aos argumentos ou como uma espécie de "força motriz" que impulsiona o debate: a do excepcionalismo da internet e a da necessidade de se atuar de forma "precaucionária", reduzindo-se os riscos.

O excepcionalismo é uma ideia que, tendo como fonte os discursos tecnodeterministas, compreende as novas tecnologias de um modo geral, e a internet em particular, como sendo algo excepcional, que do ponto de vista regulatório não pode ser tratada da mesma maneira que as demais atividades humanas objeto da regulação.

A precaução, por seu turno, constitui uma espécie de racionalidade que informa o processo de decisão quando a possibilidade de escolha das medidas regulatórias a serem empregadas. Esse princípio, apesar de ter sido inicialmente desenvolvido para ser aplicado em

[151] Tradução nossa. No original: "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."

[152] MUELLER, Milton. **Networks and States**. The global politics of internet governance. 2010.

matéria ambiental, acabou se tornando um guia geral para lidar com as situações de incerteza científica quanto aos riscos e sua influência alcançou toda a atividade regulatória. Esse fenômeno foi expressamente reconhecido na Comunicação da Comissão Europeia relativa ao princípio da precaução, quando afirma que[153]

> O princípio da precaução não é definido no Tratado, que o prescreve apenas uma vez - para proteger o ambiente. Mas, na prática, o seu âmbito de aplicação é muito mais vasto, especificamente quando uma avaliação científica objectiva preliminar indica que há motivos razoáveis para suspeitar que efeitos potencialmente perigosos para o ambiente, a saúde das pessoas e dos animais ou a protecção vegetal podem ser incompatíveis com o elevado nível de protecção escolhido para a Comunidade. [...] O recurso ao princípio da precaução constitui um elemento essencial da política comunitária e as escolhas efectuadas para este efeito repercutir-se-ão nas posições a defender a nível internacional em relação à forma como deve ser aplicado o princípio da precaução.

Assim, como forma de possibilitar uma melhor compreensão sobre a regulação da internet e das novas tecnologias, é importante que o excepcionalismo da internet e a aplicação do princípio da precaução sejam discutidas.

2.6 O EXCEPCIONALISMO DA INTERNET

Desde seus primórdios, a internet foi vista como algo único e excepcional, criado a partir de uma ideologia própria que, por sua essência fragmentada e sem fronteiras, não poderia ser objeto de regulação estatal nos mesmos moldes do que era feito em relação às demais tecnologias de comunicação. Com efeito, a criação e o desenvolvimento da internet se deram de modo peculiar. Diversamente do que aconteceu com os meios de comunicação que lhe precederam, como o telefone ou a televisão a cabo, a internet não surgiu de um empreendimento comercial desenvolvido por empresas privadas. Ao contrário, a internet começou como uma rede de pesquisas explicitamente não-comercial e pública, na qual a participação das empresas privadas se deu de forma substancialmente diversa da que ocorreu em outras mídias[154].

---

[153] COMISSÃO DAS COMUNIDADES EUROPEIAS. **Comunicação da Comissão relativa ao Princípio da Precaução,** 2000. disponível em https://op.europa.eu/pt/publication-detail/-/publication/21676661-a79f-4153-b984-aeb28f07c80a

[154] MARSDEN, Christopher. **Regulating the global internet society.** Londres: Routledge, 2000.p. 4.

Inegavelmente um dos mais importantes fatores que possibilitaram a rápida disseminação da rede mundial de computadores é que a *world wide web* foi desenvolvida como um programa de padrão aberto, tanto em relação aos direitos de propriedade quanto às possibilidades de navegação e conexão, tendo se desenvolvido a partir do trabalho de engenheiros e pesquisadores que atuavam juntos em organizações não comerciais, sob uma matriz autorregulatória. Como afirma Christopher Marsden[155], aquilo que para os usuários iniciais da internet comercial era um ato de fé (crença na possibilidade de comunicação livre e aberta, sem interferência ou controle governamental), para os governos representava a aceitação pragmática de que, para possibilitar as inovações, os modelos de regulação utilizados na internet deveriam ser tão flexíveis quanto possível, afastando-se do modelo de regulação direta anteriormente utilizado para os setores de telecomunicações ou de comunicações de massa.

Uma das consequências mais marcantes do início singular da internet foi que, como afirma Tim Wu[156], ela foi fundada com uma ideologia explícita, uma espécie de libertarianismo utópico que foi adotado pelos seus idealizadores e desenvolvedores iniciais e que até hoje ainda se faz sentir, principalmente sob a forma do tecnodeterminismo e do excepcionalismo, uma visão segundo a qual a internet, do ponto de vista regulatório, seria algo excepcional e diferente de todos os demais empreendimentos humanos.

De fato, na base dessas ideias está a noção de que a internet seria excepcional do ponto de vista regulatório, já que, por sua natureza peculiar, não poderia ser regulada através dos meios tradicionais. Há algum tempo ainda eram correntes as ideias de que o crescimento da rede levaria ao descrédito nos governos como reguladores do ciberespaço e de que as tentativas de aplicação das normas do mundo real ao mundo virtual criariam conflitos legais insolúveis[157], a ponto de alguns teóricos chegarem a sustentar que a internet seria uma realidade distinta, com sua própria soberania [158]. Essa era certamente uma posição extrema, mas, de um modo geral, era comumente aceita a ideia de que a regulação estatal da internet

---

[155] MARSDEN, Christopher. **Internet co-regulation: european Law, regulatory governance and legitimacy.** Cambridge: Cambridge University Press, 2011. P. 48

[156] WU, Tim. **Is Internet Exceptionalism Dead? .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** Washington: TechFreedom, 2010. Disponível em https://www.nyu.edu/projects/nissenbaum/papers/The-Next-Digital-Decade-Essays-on-the-Future-of-the-Internet.pdf

[157] MACCARTHY, Mark. **Internet Exceptionalism Revisited. The next digital decade - Essays on the future of the internet.** Washington: TechFreedom, 2010. Disponível em https://www.nyu.edu/projects/nissenbaum/papers/The-Next-Digital-Decade-Essays-on-the-Future-of-the-Internet.pd

[158] POST, David e JOHNSON, David. **Law and Borders–The Rise of Law in Cyberspace**, Stanford Law Review, nº 48, 1996. Disponível em http://journals.uic.edu/ojs/index.php/fm/article/view/468/82

seria muito difícil, senão impossível, o que é bem retratado pela afirmação de Bill Clinton, à época Presidente dos EUA, sobre as então incipientes tentativas da China de regular restritivamente a internet: " [...] China *is trying to crack down on the Internet – good luck. That's sort of like trying to nail Jello to the wall*"[159].

Entretanto, fatores como o "estouro" da bolha das empresas dot.com (que refreou a euforia desregulatória até então prevalente) e o ataque terrorista às torres gêmeas (que reavivou a busca por maior garantia estatal de segurança) deram início a um movimento "re-regulatório", caracterizado por uma maior intervenção estatal na regulação da internet [160], que culminou com as revelações feitas por Edward Snowden da existência de programas maciços de vigilância estatal, que contavam com a colaboração das empresas de internet.

Atualmente, a regulação da internet é um campo de batalha ideológico ainda aberto, no qual os discursos libertários e tecnodeterministas, que defendem o excepcionalismo da internet e a necessidade de que o Estado se limite a garantir a liberdade da iniciativa privada e dos usuários, disputam espaço com os discursos de viés paternalista, voltados à tutela do interesse público coletivo, que defendem a necessidade de que o Estado atue mais fortemente no controle do ciberespaço para evitar a prática de crimes e outras violações de direitos.

As discussões quanto ao caráter excepcional da internet e à necessidade de que sejam adotadas estratégias diferentes e específicas para sua regulação podem, em grande medida, ser atribuídas à geografia do ciberespaço, ou, mais propriamente, à ausência de geografia, que faz com que a ideia de exercício de poder estatal baseada o monopólio da produção do direito sobre uma base territorial definida pareça ser de alguma forma inadequada para o mundo virtual.

De fato, a internet e as tecnologias digitais desafiam o modelo tradicional de estado de direito, fundado no estabelecimento, pelas autoridades constitucionalmente competentes, de regras jurídicas que devem ser respeitadas e obedecidas por todos dentro do espaço territorial sobre o qual o estado exerce sua soberania. É inegável, portanto, a existência de uma certa tensão entre as novas mídias digitais e o estado de direito, o que levou à criação de um movimento inicial de caráter libertário e em grande medida utópico, cuja visão é muito bem retratada pela "Declaração da Independência da Internet", escrita em por John Perry Barlow, letrista do grupo Grateful Dead e um dos fundadores da Electronic Frontier Foundation , no qual ela afirmava que o ciberespaço não estava submetido às leis dos estados nacionais:

---

[159] WU, Tim. **Is Internet Exceptionalism Dead?** p. 180

[160] MARSDEN, Christopher. **Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace**. Cambridge: Cambridge University Press, 2011.

> Governos do Mundo Industrial, seus cansados gigantes de carne e aço, eu venho do Ciberespaço, a nova casa da Mente. Em nome do futuro, eu exijo a vocês do passado para nos deixar em paz. Vocês não são bem-vindos entre nós. Vocês não possuem autoridade soberana no lugar em que nos reunimos.
>
> Governos derivam seus poderes justamente do consentimento daqueles que por eles são governados. Vocês nem solicitaram ou receberam o nosso. Nós não convidamos vocês. Vocês não nos conhecem, nem conhecem o nosso mundo. O Ciberespaço não se limita às suas fronteiras. Não pensem que vocês podem construí-lo, como se fosse uma obra de construção civil. Vocês não podem. É uma força da natureza, e ela cresce através das nossas ações coletivas.
>
> Na China, Alemanha, França, Rússia, Singapura, Itália e EUA, vocês estão tentando repelir o vírus da liberdade erguendo postos policiais nas fronteiras do Ciberespaço. Isso só vai manter o contágio afastado por pouco tempo, mas eles não funcionarão em um mundo que em breve a mídia vai cobrir de bits[161].

A declaração, que foi muito compartilhada e se tornou mundialmente famosa por seu conteúdo polêmico, foi elaborada num momento histórico em que começavam os primeiros movimentos dirigidos a regular a internet, aplicando métodos regulatórios já utilizados pelo estado para o mundo real. A ligação entre as tentativas de regulação estatal e a declaração se torna ainda mais evidente quando se nota que ela foi assinada em 8 de fevereiro de 1996, mesmo dia em que então presidente americano Bill Clinton sancionou o *Communications Decency Act*[162], diploma legal que, ao mesmo tempo em que criava imunidades civis para os provedores de internet, criminalizava a divulgação de conteúdo considerado obsceno ou pornográfico para menores de 18 anos[163] o que, à época, despertou muita preocupação na comunidade da internet, que via na tentativa de regulação do ciberespaço uma manobra estatal para começar a controlar a internet.

As teses defendidas por Barlow tinham como ponto de partida a ideia de que a internet não só não deveria, mas tampouco poderia ser regulada pelos estados nacionais. Baseados no caráter anônimo da navegação na internet (já que a autenticação do usuário na rede limita-se

[161] BARLOW, John Perry. **Uma declaração da independência do ciberespaço.** Tradução de MERLO, Rafael Augusto Arruda. Disponível em http://www.mediafire.com/file/2a9pdct2kaervdp/John+Perry+Barlow+-+1996+-+Uma+Declara%C3%A7%C3%A3o+da+Independ%C3%AAncia+do+Ciberespa%C3%A7o.pdf

[162] Para uma discussão acerca das consequências da CDA na regulação da internet,.FRYDMAN, B., HENNEBEL., L. LEWKOWICZ, G.,**Public strategies for internet Co-Regulation in the United States, Europe and China.** *In* BROUSSEAU, E., MARZOUKI, M., e MËADEL, C. **Governance, Regulations and Powers on the the Internet.** Cambridge: Cambridge University Press, 2008. Disponível em HTTP://ssrn.com/abstract=1282826

[163] A parte criminal do estatuto foi julgada inconstitucional pela Suprema Corte americana, no caso Reno v. American Civil Liberties Union, 521 US 844 (1997)

ao endereço de IP da máquina utilizada, cuja identificação é meramente lógica, não física, e pode ser facilmente disfarçada com a utilização de um proxy), Barlow afirmava "Nossas identidades não têm corpos, então, diferente de vocês, nós não podemos ser forçados a seguir ordens por coerção física".

De fato, o anonimato proporcionado pela internet, aliado à inexistência de restrições para comunicações globais e instantâneas, que possibilitam o estabelecimento de negócios ou de bases de dados no exterior, tornaram significativamente mais complicada e difícil a tarefa dos estados nacionais, a ponto de os ciberlibertários assumirem a tese de que somente a autorregulação seria possível na internet, cuja natureza constituiria uma insuperável barreira à aplicação das leis[164].

O libertarianismo que marcou as origens da internet deu origem a um movimento de caráter libertário e em grande medida utópico, que defendia a ideia do excepcionalismo da internet, uma visão segundo a qual, em suma, o ciberespaço não estaria sujeito aos limites impostos pelas fronteiras entre países, e que, por isso, seria imune ao poder soberano dos estados nacionais, somente podendo ser regulado através da autorregulação, com normas criadas pela própria comunidade digital. No campo regulatório, o excepcionalismo se traduz na defesa de que as normas aplicáveis à internet sejam diferentes daquelas aplicadas ao mundo real[165].

A ideia do excepcionalismo da internet foi defendida por teóricos como David Post e David Johnson[166], que afirmavam ser o ciberespaço um local distinto do mundo real, um "não-lugar" com soberania própria, como um estado autônomo. O excepcionalismo da internet, assim, decorreria de sua própria natureza, já que ela teria sido desenvolvida como um ambiente separado, em que, diferentemente do que ocorre no mundo real, não haveria fronteiras ou meios de exercício de poder pelos estados nacionais.

Ao longo do tempo, a ideia do excepcionalismo da internet foi sofrendo modificações, de modo a se adequar às realidades trazidas pela expansão da internet comercial, com o movimento inicial, mais radical e que pregava ser a internet excepcional ao direito estatal, sendo substituído por uma versão mais comedida, para a qual o excepcionalismo estaria no

---

[164] KOZINSKI, Alex e GOLDFOOT, Josh. **A Declaration of the Dependence of Cyberspace. .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** P. 170

[165] HOLLAND, Brian. **Section 230 of the CDA:Internet Exceptionalism as a Statutory Construct. .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** P. 139 e SS.

[166] POST, David e JOHNSON, David. **Law and Borders–The Rise of Law in Cyberspace**, Stanford Law Review, nº 48, 1996. Disponível em http://journals.uic.edu/ojs/index.php/fm/article/view/468/824

caráter único da internet em relação às demais tecnologias de difusão da informação[167]. Eric Goldman[168] sustenta a existência de três ondas do excepcionalismo: a primeira foi a do *utopismo da internet*, na qual a internet foi tratada como algo realmente singular, tendo recebido um tratamento mais favorável do que o das outras mídias, como forma de garantir a inovação e a generatividade. Na década de 2000 se formou a segunda onda do excepcionalismo, denominada por Goldman de *paranoia da internet*, caracterizada pela regulação mais restritiva da internet em relação aos serviços equivalentes prestados fora do mundo virtual. Por fim, a terceira onda, iniciada por volta do início da década de 2010, é a da *proliferação do excepcionalismo*, caracterizada por uma abordagem regulatória que avança no excepcionalismo para cada nova tecnologia desenvolvida na internet.

Essa vertente do excepcionalismo é que tem ocupado espaço no debate regulatório atual, em que cada nova tecnologia desenvolvida para operar na (ou através) da internet se apresenta como disruptiva, de modo que seu caráter único e especial tornaria impossível a aplicação a ela das regras estatais pensadas para o mundo físico. Praticamente todas as novas empresas de tecnologia apresentam uma certa resistência de identificação com o já estabelecido, apresentando seu modelo de negócio como inovador, verdadeiro representante da herança schumpeteriana de destruição criativa.

Na base desse conceito é possível divisar traços do pensamento ciberlibertário, defensor da tese de que Estado não deve atuar na regulação das novas tecnologias, que somente devem estar sujeitas a alguma forma de autoregulação, a qual deverá surgir das práticas sociais e da arquitetura dos códigos[169].

Em contraponto aos excepcionalistas, no final da década de 1990 começou a ganhar corpo um movimento em sentido contrário, por alguns chamado de ciberpaternalismo, nascido a partir da percepção de que a ampla liberdade pretendida pelos ciberlibertários traria como consequência inúmeros efeitos indesejados, como a prática de crimes on line, a disseminação de imagens de abuso contra crianças e adolescentes, a proliferação de discursos de ódio, etc.

Andrew Murray[170] divide o ciberpaternalismo em duas escolas diferentes: a da *falácia da internet*, que tem como mais proeminentes representantes Jack Goldsmith e Tim Wu, para quem a internet não é mais transnacional do que outras atividades já desenvolvidas há

---

[167] CF. WU, TIM. **Is Internet Exceptionalism Dead? .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** P. 179 e ss.

[168] GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism.** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** P. 165 e SS.

[169] MUELLER, Milton. **Networks and States**. The global politics of internet governance. 2010

[170] MURRAY, Andrew. **Nodes and gravity in virtual space.**

bastante tempo, como o transporte aéreo internacional e a regulação do meio ambiente, sendo certo que em todas essas atividades houve problemas na determinação da jurisdição e das normas prevalente que foram devidamente solucionados. Ademais, argumentam que seria falaciosa a afirmação dos excepcionalistas de que na internet não seria possível aplicar as leis estatais.

Na verdade, basta notar que todos os usuários e todas as empresas que fornecem serviços na internet têm existência real, fora do mundo virtual, para facilmente se constatar que, na verdade, antes de serem imunes à jurisdição, as transações pela internet provavelmente são ainda mais sujeitas à regulação do que as praticadas fora da rede, já que potencialmente todos os países com acesso a determinada transação podem pretender regulá-la.

Um exemplo que ilustra bem a falha do argumento pela impossibilidade de regulação do ciberespaço é o que ocorreu com Julian Assange, fundador do site Wikileaks, que se apresentou como um projeto de construção de um instrumento independente de transparência mundial pela internet, que poderia se contrapor aos governos mundiais, bem na linha defendida pelos ciberlibertários e excepcionalistas. A realidade mostrou, entretanto, que passado o choque inicial, a reação dos "cansados gigantes de carne e aço" foi forte a ponto de forçar Assange a buscar proteção dentro da embaixada do Equador em Londres, onde ficou confinado para proteger-se da persecução penal.

A segunda sub-escola do ciberpaternalismo é denominada por Andrew Murray de tecno-determinista ou Berkman School, em referência ao instituto de Harvard de onde vieram os autores mais proeminentes dessa escola. Essa linha do ciberpaternalismo defende a ideia de que o excepcionalismo da internet decorre não de sua natureza específica, mas de um fenômeno regulatório e cultural. Para Lawrence Lessig, principal expoente dessa escola, tudo o que torna a internet única (no sentido libertariano) decorre de escolhas feitas nos códigos de programação, e não de algo que esteja em sua essência.

O excepcionalismo, pelo menos em sua vertente mais radical, que defendia a impossibilidade da regulação estatal da internet, é hoje um movimento quase que somente de interesse histórico. A questão é diferente, entretanto, no que diz respeito às posições mais comedidas do excepcionalismo, que defendem o caráter único e excepcional da internet não em relação ao direito e à possibilidade de regulação estatal, mas em relação às outras mídias, aos outros meios de comunicação de massa. Essa versão do excepcionalismo, assim, defende a necessidade de que as normas aplicáveis à internet sejam diferentes daquelas aplicáveis às atividades congêneres realizadas no mundo real.

As posições excepcionalistas em grande medida se fundamentam no paradigma tecnodeterminista, que apresenta as novas tecnologias como sendo unicamente resultado da evolução da técnica e da Ciência, cujo desenvolvimento irá melhorar a vida das pessoas e da sociedade. Essa versão do excepcionalismo parte da ideia de que, por se tratar de uma evolução técnica e científica, seu estatuto jurídico não pode ser o mesmo aplicado a situações análogas fora do ciberespaço, sob pena de inviabilizar-se o progresso.

Vale notar que o discurso tecnodeterminista é muito eficiente como fundamentação do excepcionalismo da internet, já que, uma vez excluídas do discurso as implicações sociais concretas das tecnologias, restam como objeto de análise unicamente as inovações e suas maravilhas, contra as quais ninguém pode ser contrário.

Este tipo de abordagem ainda tem muita força no campo da regulação da internet, especialmente quando se pensa na regulação feita pelo Poder Judiciário, onde ainda têm muita força os argumentos que defendem o caráter único e excepcional da internet, não em relação ao Direito e à possibilidade de regulação estatal, mas em relação às outras mídias, aos outros meios de comunicação de massa ou a serviços análogos existentes no mundo real.

Quando assumem essa forma, as ideias excepcionalistas ainda são bastante prevalentes nas discussões sobre governança da internet, especialmente fora dos espaços de discussão mais técnicos. Kozinski e Goldfoot[171] mostram como ainda é comum na jurisprudência norte-americana a adoção de posições excepcionalistas na solução de casos relacionados com a regulação da internet.

No Brasil, a questão está em vias de ser apreciada pelo Supremo Tribunal Federal, na Ação Direta de Inconstitucionalidade 5613, atualmente sob a relatoria do Min. Nunes Marques, que foi proposta em outubro de 2016 pela Associação Brasileira de Jornais com o objetivo de que seja conferida interpretação conforme a alguns artigos da lei 10.610/2002, de modo que "a regulação legal a que se sujeitam os veículos de comunicação tradicionais (radiodifusores e impressos) se aplica, igualmente, a portais de notícias na internet"[172].

A questão central a ser decidida no processo, portanto, refere-se exatamente à tese excepcionalista moderada, já que o objetivo da ANJ é a de garantir que portais de notícias na internet se submetam às mesmas regras que os demais veículos de comunicação em massa. Para os autores da ação, "a sujeição dos portais da internet à disciplina constitucional e legal

[171] KOZINSKI, Alex e GOLDFOOT, Josh. **A Declaration of the Dependence of Cyberspace. .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** P. 170

[172] CARNEIRO, Luiz Orlando. Portal Jota. disponível em https://jota.info/justica/capital-estrangeiro-anj-pede-ao-stf-que-portais-de-noticias-na-internet-sejam-equiparados-jornais-impressos-20102016

aplicável às empresas jornalísticas impõe-se também em razão das características da própria rede mundial de computadores, que potencializa a disseminação de notícias".

Vale notar que, mesmo a despeito de ainda não ter havido decisão específica quanto à questão pelo STF, a Corte, no julgamento da ADPF 130, em que se discutia a recepção da lei de imprensa pela Constituição Federal de 1988, deu indicações de que adotaria a tese do excepcionalismo da internet, ao afirmar que, ante o silêncio da Constituição quanto ao seu regime, a internet deve ser entendida como "território virtual livremente veiculador de ideias e opiniões, debates, notícias e tudo o mais que signifique plenitude de comunicação", não podendo ser incluída no conceito de "imprensa" para efeito de tratamento legal. Segundo o voto condutor do julgamento,

> Ficando de fora do conceito de imprensa, contudo, por absoluta falta de previsão constitucional, a chamada "Rede Mundial de Computadores - INTERNET". Artefato ou empreitada tecnológica de grandes e sedutoras possibilidades informativas e de relações interpessoais, sem dúvida, dentre elas a interação em tempo real dos seus usuários; ou seja, emissores e destinatários da comunicação internetizada a dispor da possibilidade de inverter as suas posições a todo instante. O fisicamente presencial a cada vez mais ceder espaço ao telepresencial (viagem que vai do concreto ao virtual), porém, ainda assim, constitutivo de relações sem a menor referência constitucional. O que se explica em função da data de promulgação da Carta Política brasileira (5 de outubro de 1988), quando os computadores ainda não operavam sob o tão refinado quanto espantoso sistema eletrônico-digital de intercomunicação que veio, com o tempo, a se chamar de "rede".[173]

Vale notar que, antes de ter sido levada ao STF, a questão havia sido objeto de representação feita pela Associação Brasileira de Emissoras de Rádio e Televisão (ABERT) e pela Associação Nacional de Jornais (ANJ) à Procuradoria da República no Rio Grande do Sul contra o portal Terra Networks Brasil S.A.(TERRA), por suposta violação ao § 1º do art. 222 da Constituição Federal. Na peça, as representantes alegaram que mais de 30% do capital social do portal Terra pertenceriam a estrangeiros (a espanhola Telefônica), violando a Constituição e a lei 10.610/2002.

A representação, que deu origem ao procedimento 1.29.000.001082/2010-16, foi arquivada pela Procuradoria da República em 2010, sob o fundamento de que "não se vislumbra lesão a direito consumerista nem infração à ordem econômica"[174], tendo sido a

[173] SUPREMO TRIBUNAL FEDERAL, ADPF 130. Rel. Min. Ayres Britto. p. 27/28

[174] As informações relativas ao procedimento foram extraídas do voto da relatora, Subprocuradora Raquel Dodge, disponível em http://s.conjur.com.br/dl/terra-anj-voto-raquel-dodge-csmpf.pdf, e do voto vista do

promoção de arquivamento encaminhada para a 3ª Câmara de Coordenação e Revisão (3a. CCR) do MPF para homologação.

Apreciando a matéria, a 3a. CCR, rejeitou a tese da excepcionalidade da internet, recusando a homologação do arquivamento e determinando o retorno do procedimento à origem, para que fosse proposta ação civil pública. Na decisão ficou consignado que

> Analisando a questão sob o ponto de vista da natureza do serviço, uma empresa que atue como portal de conteúdo na internet não pode ser tratada de forma equivalente aos jornais, as emissoras de rádio e de televisão, dada sua especificidade e o fato de a internet se constituir num ambiente descentralizado e sem fronteiras.

O portal Terra interpôs recurso ao Conselho Institucional do Ministério Público Federal, mais alto órgão de solução de controvérsias administrativas no *Parquet* federal, que decidiu pelo arquivamento do procedimento, expressamente recorrendo a argumentos ligados ao caráter único e excepcional da internet. Para a melhor compreensão das posições antagônicas, vale transcrever trecho da fundamentação do voto da relatora, favorável à continuidade das investigações (e, por consequência, contrária à tese excepcionalista):

> O risco de que a manifestação do pensamento, a criação, a expressão e a informação sob qualquer forma, processo ou veículo sofra restrição que se subtraia à proteção constitucional, por falta de meio para contê-la ou puni - la, não acontece apenas quando a empresa jornalística utiliza o papel ou meio físico semelhante. O risco é ainda maior quando o meio é eletrônico. O escopo constitucional quando estabelece tal restrição ao direito de propriedade é o de proteger estes bens jurídicos

O voto vencedor, por seu turno, indicou que, em razão de todas as especificidades da internet, as restrições do art. 222 da CF, previstas para as empresas jornalísticas, não se aplicam aos portais de notícias na internet.

A análise do procedimento no âmbito do Ministério Público e dos fundamentos utilizados para sua resolução demonstram a força dos argumentos excepcionalistas, que são apresentados como sendo verdades auto-evidentes. A afirmação do caráter único e excepcional da internet, decorrente de sua "geografia" e da ausência de fronteiras, foi suficiente para a definição da questão, sem que houvesse qualquer discussão acerca da regulabilidade da rede. Alguém que se deparasse com os argumentos apresentados em favor

---

Subprocurador Mario Luiz Bonsaglia, disponível em https://jornalggn.com.br/sites/default/files/documentos/voto_vista_1082.pdf

da imunidade dos portais de notícias às normas constitucionais poderia facilmente ser levado a crer que o argumento vinha de um defensor do ciberlibertarianismo.

O problema deste tipo de abordagem, que não leva em conta a evolução da discussão acerca da regulabilidade da internet e a incrustação do desenvolvimento das tecnologias às relações sociais e econômicas, é que ele abre margem à tomada de decisões voluntaristas e tecnicamente frágeis, que trazem um duplo risco.

O primeiro é o de não ser capaz de efetivamente tutelar os direitos fundamentais dos cidadãos ante os possíveis riscos das novas mídias digitais, inclusive aqueles decorrentes da concentração de poder nas mãos das empresas que definem os códigos e, assim, têm em mãos ampla possibilidade de exercer controle perfeito da atividade.

O outro risco é o de permitir atuações regulatórias voluntaristas e autoritárias que, por não compreenderem corretamente as limitações e os condicionantes da tecnologia (e da regulação pela arquitetura), imponham soluções que podem causar aumento na insegurança e perda da eficiência ou por em risco a generatividade da rede.

A regulação da internet e das aplicações que a utilizam é, no atual estágio de desenvolvimento da tecnologia, não só um tecnicamente possível, mas constitui também uma necessidade inegável. A utilização de uma concepção ampla de regulação permite compreender melhor as forças regulatórias que atuam na internet, possibilitando que a dogmática jurídica analise o fenômeno a partir de suas bases reais, e nele atue de modo a efetivamente poder guiar as práticas regulatória.

Assim, a questão que realmente tem relevância atualmente não é mais se a internet pode ser regulada, mas sim como deve ser feita essa regulação para que o interesse público efetivamente seja protegido. Por isso, é preciso superar a visão de que a atividade regulatória deve se ater unicamente à busca por soluções de falhas de mercado, uma vez que a tutela de direitos fundamentais sem conteúdo econômico direto é também um objetivo da atividade regulatória.

As posições ciberlibertárias, mesmo em suas versões mais comedidas, que advogam um tratamento excepcional para os aplicativos e serviços na internet, diverso daquele conferido a produtos e serviços análogos fora do ciberespaço, não podem mais se sustentar unicamente em argumentos de natureza tecnodeterminista. Ao contrário, é preciso que em cada um dos casos seja discutido e analisado concretamente não só os aspectos relevantes e inovadores das novas tecnologias, mas principalmente quais suas implicações e efeitos concretos. Somente a partir de uma tal abordagem seria possível legitimamente pretender um tratamento excepcional.

Por outro lado, não se pode perder de vista o fato de que as forças que atuam na elaboração dos códigos são também produtos sociais e que inexiste algo como uma "essência" da internet ou das tecnologias criadas. Todas as forças regulatórias (código, leis, costumes e mercado) interagem continuamente, uma interferindo nos limites e conteúdos impostos pelas demais, por isso que é preciso reconhecer que a regulação não é feita unicamente pela normas editadas pelos agentes regulatórios, já que esse papel é também desempenhado pela escolha e definição de questões de natureza eminentemente técnica (basta lembrar da arquitetura fim-a-fim da internet e as consequências que a escolha por tal modelo gera em termos de fragmentação e impossibilidade de controle centralizado de conteúdo na rede), econômica (o que é bem demonstrado pelas consequência da economia de dados baseada no capitalismo de vigilância, com modelos de negócio em que o serviço é disponibilizado de forma gratuita em troca da possibilidade de obtenção de dados pessoais para serem tratados e comercializados com terceiros), e, finalmente, os costumes (por exemplo, essa cultura de extrema visibilidade e exposição de situações que até pouco tempo era tido como privadas fornecem um ótimo exemplo).

A compreensão da regulação das novas tecnologias, portanto, não pode ser limitada à análise das leis e normas, mas constitui uma matéria extremamente complexa. Aliás, vale lembrar que além da regulação da internet resultar de uma multiplicidade de fatores, esses fatores se relacionam entre si, influenciando-se mutuamente em uma relação dialética onde, por exemplo, as leis condicionam a atuação do mercado, o mercado direciona o desenvolvimento das tecnologias e dos códigos, os algoritmos (códigos) estimulam o desenvolvimento de costumes e esses, por seu turno, influenciam a edição de leis e normas regulatórias, sendo certo que esse "fluxo" de interações é meramente exemplificativo, uma vez que as posições ocupadas por quaisquer dos fatores pode ser livremente alterada, já que todos interagem e se influenciam simultaneamente.

Esse plexo de interações que ao mesmo tempo conformam, estimulam, limitam, condicionam e orientam o desenvolvimento das novas tecnologias é resultado de toda a organização social em que estamos imersos, em que o papel da tecnologia assume posição de excepcional relevância e onde as relações sociais passam a ser mediadas pela ideia do risco anônimo nas relações, decorrente da crescente complexização e especialização. Por suas implicações no campo regulatório, onde impulsiona uma abordagem precaucionária, vale a pena revisitar aqui a ideia da sociedade do risco como modelo da atual organização social.

A conceituação da atual organização social como uma sociedade do risco é obra do sociólogo Ulrich Beck[175], para quem a modernidade baseada em estados-nação foi implodida por algumas consequências imprevistas da modernização: a globalização, a individualização, a revolução feminina, o subemprego e os riscos globais (como a crise ecológica e o colapso dos mercados financeiros). Cria-se, assim, um novo modelo de sociedade, onde o inimigo definido (especialmente aquele identificado no conflito entre ocidente e oriente, entre capitalismo e socialismo e entre pobres e ricos) cede espaço ao risco generalizado. Para Beck,

> O acúmulo de poder do progresso tecnológico-econômico é cada vez mais ofuscado pela produção de riscos. Estes somente se deixam legitimar como "efeitos colaterais latentes" num estágio inicial. Com sua universalização, escrutínio público e investigação (anticientífica) eles depõem o véu da latência e assumem um significado novo e decisivo nos debates sociais e políticos. [...] No centro da questão estão os riscos e efeitos da modernização, que se precipitam sob a forma de ameaças à vida de plantas, animais e seres humanos. Eles já não podem – como os riscos fabris e profissionais do século XIX e na primeira metade do século XX – ser limitados geograficamente ou em função de grupos específicos.[176]

Os novos riscos criados pela sociedade pós-industrial, a sociedade de risco, distinguem-se daqueles anteriormente criados nas sociedades industriais por não poderem ser delimitados local, temporal, nem socialmente. Na realidade, os novos riscos não estão restritos a um único grupo ou classe social, mas distribuem-se por toda sociedade, mesmo aqueles não diretamente envolvidos na atividade geradora do risco. Tampouco é possível estabelecer-se uma relação de causa e efeito direta entre a atividade e o dano, pelo que a fórmula clássica de responsabilização e atribuição de culpa não se mostram suficientes. Por fim, dada a irreversibilidade de seus efeitos, tais riscos não podem ser propriamente compensados ou revertidos, por isso que a precaução ganha espaço cada vez maior como técnica de gestão de riscos.

O conceito de sociedade de risco foi formulado por Beck em obra de 1986, antes mesmo da criação da internet, entretanto o diagnóstico de uma sociedade globalizada e permeado por macroperigos generalizados, que não são temporal ou geograficamente limitados, cujos responsáveis não podem ser corretamente individualizados e que são praticamente irreversíveis pode ser bastante útil como ferramenta para identificar algumas das circunstâncias que se mostraram essenciais para a ampla disseminação da vigilância que

---

175 BECK, Ulrich. **Sociedade de risco. Rumo a uma outra modernidade**. Trad. Sebstião Nascimento. SÃO PAulo: Editora 34, 2010. P. 2

176 IDEM IBIDEM. P. 15-16.

conforma a atual sociedade da informação. Não há, portanto, qualquer contraposição entre as ideias de sociedade de risco e de sociedade da informação, mas na realidade os conceitos se complementam, já que, como afirmou Beck[177],

> É precisamente com o avanço da sociedade de risco que se desenvolvem como decorrência as oposições entre aqueles que são afetados pelos riscos e aqueles que lucram com eles. Da mesma forma, aumenta a importância social e política do conhecimento, e consequentemente do acesso aos meios de forjar o conhecimento (ciência e pesquisa) e disseminá-lo (meios de comunicação de massa). A sociedade de risco é, nesse sentido, também a sociedade da ciência, da mídia e da informação.

A sociedade de risco é um aspecto da sociedade que desenvolveu a tecnologia a ponto de tornar as relações sociais e os riscos indetermináveis e não mais restritos e, por isso, cria as condições ideias para a difusão de uma sensação generalizada de medo, que, por seu turno, alimenta o desejo difundido na sociedade de controlar o futuro, reduzindo riscos. Nessa perspectiva, a sociedade de risco, embora não seja objetivamente mais perigosa do que outros modos de organização social preexistentes, constitui um modelo de organização em que prevalece a noção subjetiva de que o mundo se tornou mais perigoso (ainda que essa percepção não seja verdadeira). Por isso, como bem resumiu Giddens[178], a sociedade de risco é "uma sociedade cada vez mais preocupada com o futuro (e também com a segurança)"

Nesse modelo de sociedade, toda a atividade regulatória acaba de alguma forma sendo pensada a partir da noção de que há necessidade de endereçar adequadamente o tratamento e a gestão de riscos, por isso que a abordagem precaucionária que assume grande importância como fundamento da atuação regulatória na edição de leis e normas.

De fato, a percepção subjetiva da população acerca dos riscos anônimos e não restritos gera uma crescente sensação de insegurança social que, por seu turno, gera uma grande pressão sobre toda a atuação dos reguladores, que passa a ser mais voltada à garantia de segurança, por isso a precaução assume papel de extrema importância nas estratégias regulatórias.

---

[177] BECK, Ulrich. **Sociedade de risco. Rumo a uma outra modernidade**. Trad. Sebastião Nascimento. São Paulo: Editora 34, 2010. P. 56

[178] GIDDENS, Anthony; PIERSON, Christopher. **Conversas com Anthony Giddens: o sentido da modernidade**. Trad. Luiz Alberto Monjardim. Rio de Janeiro: Editora FGV, 2000, p. 142.

2.7 O PRINCÍPIO DA PRECAUÇÃO NA REGULAÇÃO

O desenvolvimento das novas tecnologias, especialmente a internet, o *big data* e a inteligência artificial, acarreta inegavelmente uma série de novos riscos globalmente distribuídos e acerca dos quais cada vez mais as pessoas passam a estar conscientes. Assim, numa análise acerca da regulação de tais tecnologias, talvez a mais premente questão que se coloca seja a relativa à forma como o estado regulador deve agir quando ainda não ainda não é possível se antever de forma clara quais serão os possíveis danos a serem causados por essa tecnologia, ou mesmo se eles efetivamente existirão.

Especificamente em relação aos riscos das novas tecnologias, tornou-se lugar comum a afirmação de que os dados são o novo petróleo. Essa analogia foi criada pelo matemático e cientista de dados britânico Clive Humby em 2006, tendo alcançado grande repercussão em 2017, quando a Reportagem de capa da The Economist[179] afirmou que o recurso mais valioso do mundo não era mais o petróleo, e sim os dados. Essa analogia significa fundamentalmente que, da mesma forma que o petróleo foi o recurso natural que sustentou a segunda revolução industrial, permitindo o surgimento e a expansão dos motores a combustão, a geração de energia e a indústria química e de explosivos, no contexto da quarta revolução industrial os dados passam ser o recurso mais valioso e importante para a economia.

Essa abordagem no mais das vezes reflete uma perspectiva tecnodeterminista, que implica uma visão extremamente benevolente e otimista do desenvolvimento tecnológico, que encontra um exemplo marcante no relatório *Data Science in the new economy: a new race for talent in the fourth industrial revolution*, publicado pelo Fórum Econômico mundial em julho de 2019[180], no qual são reafirmadas as promessas de um futuro melhor para os trabalhadores do mundo inteiro, que no longo prazo seriam beneficiados pela substituição da atividade humana braçal pela tecnologia e pelo aumento da procura por profissionais qualificados da área de tecnologia e análise de dados.

Do ponto de vista econômico, há evidente falhas na comparação entre dados e o petróleo. De início os dados não são um recurso finito e cuja escassez e dificuldade de obtenção desempenham um papel extremamente importante em sua escala de valor, como o petróleo. Na verdade, os dados, apesar de serem privados, podem ser facilmente replicados e

[179]THE ECONOMIST. Edição de 06 de maio de 2017. Disponível em : https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[180] WORLD ECONOMIC FORUM. **Data science in the new economy: a new race for talent in the fourth industrial revolution.** Julho de 2019. disponível em https://www.weforum.org/reports/data-science-in-the-new-economy-a-new-race-for-talent-in-the-fourth-industrial-revolution

reutilizados, de modo que constituem bens não rivais, no sentido de que sua utilização por alguém não impede ou diminui a possibilidade de que outras pessoas os utilizem também[181]. Além disso, ao contrário do petróleo, os dados não têm um valor objetivamente mensurável, já que seu valor depende de inúmeros fatores. O mesmo conjunto de dados pode ser valorado de forma diferente, seja pelos seus titulares, seja por aqueles que irão fazer seu tratamento e análise. Assim, ao contrário do petróleo, que tem cotação uniforme no mercado internacional, os dados têm valor diferente a depender da pessoa e do uso a que se destinam.

A analogia entre petróleo de dados, entretanto, pode ser extremamente útil para ajudar a pensar o regime de gestão de riscos associado à exploração de dados. Em um instigante artigo, Dennis Hirsch[182] apresenta um novo olhar a analogia entre dados e petróleo, focada nos aspectos negativos dessas atividades, onde sustenta ser possível se valer dessa analogia para, a partir das soluções criadas para a poluição e o efeito estufa causados pelo petróleo, pensar estrategicamente os riscos relacionados à privacidade que a massificação do uso de dados gera.

Hirsch ressalta o poder das analogias não só como instrumentos para a compreensão de problemas contemporâneos, mas também como forma de possibilitar o desenvolvimento de soluções para eles, a partir da adaptação de ideias e soluções utilizadas em problemas anteriores para o contexto atual. Nesse sentido, a analogia entre dados e petróleo funciona muito bem para endereçar os riscos porque há muita similaridade nos riscos gerados por essas duas atividades. Segundo ele,

> À medida que os conjuntos de dados aumentam, a ameaça também cresce. Big Data é como um enorme petroleiro navegando em cardumes de hackers, criminosos e erros humanos. Pode nos tornar mais inteligentes e mais ricos e nossas vidas melhores. No entanto, como o petróleo, também pode nos prejudicar. A lei ambiental desenvolveu maneiras de reduzir a poluição por óleo. Este artigo baseia-se nessa história de sucesso da lei ambiental para identificar maneiras pelas quais a lei e a política podem proteger a privacidade na era do Big Data[183].

[181] MANKIW. Gregory. **Introdução à economia.** São Paulo: Cengage Learning, 2009. p. 204

[182] HIRSCH, Dennis D., **The Glass House Effect: Big Data, The New Oil, and the Power of Analogy**, Maine Law Review, Vol. 66, 2014. Disponível em: https://digitalcommons.mainelaw.maine.edu/mlr/vol66/iss2/3

[183] Tradução nossa. No original: "As the data sets get larger, the threat grows as well. Big Data is like a massive oil tanker navigating the shoals of hackers, criminals and human error. It can make us smarter and wealthier and our lives better. However, like oil, it can also harm us. Environmental law has developed ways to reduce oil pollution. This article draws on this environmental law success story to identify ways that law and policy can protect privacy in the era of Big Data."

De fato, os principais riscos à vida humana e ao meio ambiente gerados pela atividade petrolífera são os *vazamentos* de óleo na extração, transporte ou armazenamento do petróleo e a *mudança climática* gerada pelo efeito estufa. Para ambas as categorias de risco o direito, especialmente o ambiental, vem criando meios de controlar a atividade de modo a preservar as condições de vida no planeta.

Os riscos causados pelo tratamento de dados na sociedade da informação podem ser agrupados nessas duas categorias. Na primeira, estariam os riscos de *vazamento* de dados, ocasionando insegurança nas operações comerciais e bancárias, possibilitando a ocorrência de roubo de identidades, fraudes, ameaças e violação à dignidade dos titulares de dados. Por outro lado, uma outra categoria de riscos seria a relacionada à criação de um mundo em que a constante exposição e a impossibilidade de manutenção de um espaço privado geram efeitos deletérios para o livre desenvolvimento da personalidade humana, criando uma sociedade onde todos estão sujeitos a vigilância constante. Traçando um paralelo com as mudanças climáticas causadas pela emissão de carbono, que causam o efeito estufa, Hirsch fala em um *efeito casa de vidro,* que seria decorrente da surveillance e do tratamento de dados, fazendo, no original em inglês, um jogo de palavras entre *greenhouse effect* (efeito estufa) e *glass house effect* (efeito casa de vidro).

Essa abordagem também tem a grande virtude de ressaltar a importância de que os riscos associados à mudança geral do panorama de tratamento de dados sejam bem percebidos. Do ponto de vista da atividade regulatória, essa percepção tem gerado uma profunda mudança de atitude, que foi denominada de revolução copernicana na proteção de dados, que tem deixado de se centrar na autodeterminação informativa e passa a se centrar cada vez mais no gerenciamento dos riscos das atividades de tratamento de dados[184] .

Trata-se de um processo em que emergem mecanismos mais centrados na identificação e mitigação das incertezas ainda existentes quanto às consequências concretas das atividades de tratamento ante os indivíduos, por isso que não se cuida aqui de simplesmente superar ou abandonar princípios como o da autodeterminação informativa, mas unicamente de se reconhecer a existência de uma nova moldura teórica a ser utilizada na regulação das novas tecnologias, que foi acolhido na elaboração do Regulamento Europeu de Proteção de dados e na Lei Geral de Proteção de dados brasileira.

---

[184] BIONI, Bruno e MARIA, Luciano. **O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o Seu Portal de Entrada?** Em FRAZÃO, ANA e MULHOLLAND, Caitlin. **Inteligência artificial e direito.** São Paulo: Revista dos Tribunais, 2020. Disponível em https://brunobioni.com.br/home/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf

Esse novo paradigma no tratamento da proteção de dados levou a uma guinada da "autodeterminação informacional", fundada na proteção de dados pessoais, em direção de uma abordagem mais ampla, fundada na gestão dos riscos produzidos pela informação, uma abordagem que compreende os riscos como qualquer consequência negativa do processamento de dados, tanto para o indivíduo quanto para a coletividade. Como afirmam Bioni e Maria, "o saldo normativo das novas leis de proteção de dados pessoais é resultado cada vez mais de uma arquitetura precaucionária de danos."[185]

A resposta mais usualmente apresentada para os processos fundados na gestão e prevenção de riscos é a baseada nas ideias de prudência, cuidado e responsabilidade ante o desconhecido. Trata-se do princípio da precaução, que em sua formulação mais difundida afirma que as autoridades devem adotar medidas de proteção contra potenciais danos, ainda que não existam evidências conclusivas quanto ao nexo causal entre a atividade e o dano ou mesmo de que o dano efetivamente irá ocorrer.[186]

Os termos simples em que foi formulado tal princípio, que reflete a ideia muito difundida segundo a qual "é melhor prevenir do que remediar", aliado ao fato de que ele parece fornecer um parâmetro decisório que evita as crescentes tecnicalidades inerentes às discussões regulatórias, fez com que a sua força e a influência crescesse exponencialmente, a ponto de ter se tornado hoje não só o mais importante dos princípios do direito ambiental[187], mas também ter se transformado na base de toda a política regulatória[188], assumindo papel central como parâmetro a ser seguido na regulamentação das atividades humanas potencialmente danosas à saúde, à segurança e ao meio ambiente. Ambiental, espraiando sua influência até mesmo no campo do direito penal.

Entretanto, a aplicação do princípio da precaução ao desenvolvimento das novas tecnologias não é algo simples, na medida em que esta questão está relacionada, em última análise, à própria decisão acerca da gestão dos riscos da atividade, ou seja, à definição de quem deverá, ao final, arcar com os prejuízos eventualmente causados pelas novas tecnologias. Ademais, trata-se de um campo em constante mutação, onde as modificações se sucedem em uma velocidade assombrosa, o que contribui para ampliar ainda mais as dificuldades analíticas.

---

[185] Op. Cit., p. 9.

[186] SUNSTEIN, Cass. **Laws of fear: beyond precautionary principle.** Cambridge: Cambridge University Press, 2005, p.4

[187] O'RIORDAN, Timothy e JORDAN, Andrew. **The precautionary principle, science, politics and ethics. Centre for Social and Economic Research on the Global Environment**. Working Paper PA 95-02 . Disponível em http://cserge.ac.uk/sites/default/files/pa_1995_02.pdf. p. 3

[188] SUNSTEIN, Cass. **Para além do princípio da precaução**. Revista de Direito Administrativo, V. 259. Rio de Janeiro: Ed. Revista dos Tribunais, 2012, p. 14.

Nas últimas décadas popularizaram-se as noções de que as atividades humanas podem representar risco à manutenção das condições de vida na terra e de que as atuais gerações têm responsabilidade para com as gerações futuras. Tais ideias, ligadas à equidade intergeracional, têm sido aceitas sem controvérsia relevante não só pelos movimentos sociais ambientalistas, mas também por governos e organismos multilaterais em todo o mundo[189], que as têm utilizado como fundamento para a limitação das atividades humanas de modo a buscar assegurar que o desenvolvimento atenda às necessidades do presente sem comprometer a capacidade das gerações futuras de atenderem às suas próprias necessidades.

O compromisso com as gerações futuras, assumido pelos responsáveis pelas políticas públicas, todavia, impõe necessariamente a tomada de decisões em contextos de incerteza quanto aos possíveis danos decorrentes de produtos ou atividades humanas. É certo que todas as atividades humanas envolvem algum nível de risco. Alguns riscos são bastante conhecidos e bem documentados estatisticamente, como aqueles inerentes à circulação de veículos. Outros, entretanto, estão ainda numa zona de incerteza científica não só quanto à probabilidade de sua ocorrência, mas até mesmo quanto à sua existência (v.g. os supostos danos decorrentes da radiação eletromagnética de antenas de celular). A regulação de uma atividade com vistas à redução dos riscos sempre envolve uma análise de probabilidades e, uma vez que nunca é possível afastar por completo a possibilidade de dano, toda decisão sobre o futuro é tomada em um contexto de incerteza[190].

Releva notar que na atual configuração social, os riscos são difusos e assumem um caráter estrutural, sendo que os macroperigos ecológicos, nucleares, químicos e genéticos se caracterizam por uma tripla negativa: não são delimitados temporal ou espacialmente, não podem ser imputados a um indivíduo e são irreversíveis, não podendo ser compensados ou indenizados[191]. Nestas condições, ganha especial relevo a questão de como devem decidir os responsáveis pela regulação das atividades naqueles casos em que a ciência não pode determinar com segurança o grau de risco de um produto ou de uma atividade.

As primeiras previsões normativas do princípio da precaução se deram na lei de proteção ambiental sueca de 1969[192] e na prática administrativa da Alemanha Ocidental das décadas de 1970 e meados de 1980, quando o governo passou a adotar regras mais rigorosas

---

[189] O'RIORDAN e JORDAN. Op. Cit.

[190] WIENER, Jonathan. **Precaution in a multirisk world.** Duke Law School Public Law and legal Working Paper, 2002. Disponível em: http://scholarship.law.duke.edu/faculty_scholarship/1113. p. 1511 e ss

[191] BECK, Ulrich. **A Política Na Sociedade de Risco.** Revista eletrônica Ideias – Unicamp - v. 1, n. 1, 2010. Disponível em http://www.ifch.unicamp.br/ojs/index.php/ideias/article/view/66/62, p. 230.

[192] SUNSTEIN, Cass. **Laws of fear: beyond precautionary principle.** Cambridge: Cambridge University Press, 2005, p. 17

para combater a chuva ácida, a poluição do Mar do Norte e o aquecimento global, mediante a imposição da obrigatoriedade de que as atividades potencialmente nocivas adotassem a melhor tecnologia disponível para minorar tais riscos, com base no *vorsorgeprinzip* (princípio da precaução). Desde então, o princípio foi incorporado em inúmeros acordos e tratados internacionais e nos ordenamentos internos de diversos países[193].

Entretanto, apesar de sua imensa disseminação, a implementação do princípio da precaução está longe de ser incontroversa, a começar pelo fato de que reina ainda grande indefinição quanto à sua conceituação, seus fundamentos e aplicações possíveis. Jonathan Wiener[194] aponta a existência de um levantamento que encontrou 19 formulações diferentes para o princípio da precaução, algumas das quais contraditórias entre si.

A falta de cuidado analítico e a vagueza na definição do princípio e de suas hipóteses de aplicação foi realçada por Richard Stewart[195], para quem é possível identificar 4 concepções principais nas quais seria possível encaixar as diversas versões de princípio da precaução encontrados em diplomas normativos, na literatura acadêmica e em processos judiciais:

> 1) A incerteza científica quanto ao risco de uma atividade potencialmente danosa não pode impedir sua regulamentação (precaução como não exclusão);
>
> 2) Os controles regulatórios de uma atividade devem incorporar uma margem de segurança, limitando-se a atividade a um nível abaixo do qual não tenham sido observados ou previstos efeitos adversos (precaução como margem de segurança);
>
> 3) Atividades que apresentem um potencial desconhecido de causar dano significativo devem se sujeitar à utilização da melhor tecnologia disponível, a não ser que o interessado demonstre que elas não apresentam risco considerável (precaução como melhor tecnologia disponível);

---

[193] O'RIORDAN, Timothy e JORDAN, Andrew. **The precautionary principle, science, politics and ethics. Centre for Social and Economic Research on the Global Environment**. p. 15

[194] WIENER, Jonathan. **Precaution in a multirisk world.** Duke Law School Public Law and legal Working Paper, 2002. Disponível em: http://scholarship.law.duke.edu/faculty_scholarship/1113. p. 1513

[195] STEWART, Richard B. **Environmental regulatory decisionmaking under uncertainty**. University College London Symposium on the Law & Economics of Environmental Policy, 2001. Disponível em http://www.ucl.ac.uk/cserge/Stewart.pdf

> 4) Atividades cujo risco de dano significativo seja incerto devem ser proibidas até que o interessado demonstre que elas não representam perigo (precaução como proibição).

É possível divisar a existência de uma gradação entre as diferentes versões, que vão desde aquelas mais fracas, nas quais o princípio da precaução limita-se a justificar a possibilidade de restrição a atividades potencialmente danosas, mesmo que ainda seja incerto o perigo, até versões mais fortes, onde a incerteza quanto à absoluta segurança da atividade ou do produto (cuja prova é ônus do empreendedor) deve levar à total proibição. Exemplo da versão fraca é o texto do princípio 15 da declaração do Rio, segundo o qual "quando houver ameaça de danos sérios ou irreversíveis, a ausência de absoluta certeza científica não deve ser utilizada como razão para postergar medidas eficazes e economicamente viáveis para prevenir a degradação ambiental".

Por outro lado, o protocolo de Cartagena sobre biossegurança[196], que autoriza os países signatários a rejeitarem carregamentos de organismos geneticamente modificados vindos de outros países, caso acreditem serem eles inseguros, mesmo sem evidências científicas, é um bom exemplo da utilização de uma formulação mais forte e restritiva do princípio da precaução. Outro exemplo pode ser encontrado na Carta Mundial para a Natureza, adotada pela Assembleia Geral da ONU e que, em sua Seção II, 11 (B), prevê que "as atividades que possam representar risco significativo para a natureza devem ser precedidas de uma análise exaustiva, seus proponentes devem demonstrar que os benefícios esperados superam possíveis danos à natureza, e onde os potenciais efeitos adversos não são completamente compreendidos, as atividades não devem prosseguir".

Para Frank Cross[197], o princípio da precaução é aplicado de forma unidimensional, o que faz com que a análise de risco seja focada em uma única específica fonte de risco, aquela objeto de regulação. Ademais, ao focar-se em novos riscos, a aplicação do princípio da precaução acaba por perpetuar os riscos antigos. O autor defende que as autoridades encarregadas da regulação devem confrontar a incerteza científica com prudência, utilizando-se de todo o conhecimento científico disponível para definir a conduta adequada, o que requer

---

[196] Sobre a formulação forte do princípio da precaução no protocolo de Cartagena sobre Biossegurança, ver GOKLANY, Indur. **Precaution without perversity: a comprehensive application of the precautionary principle to genetically modified crops.** Biotechnology Law Report, Vol. I, n. 3, PP. 377-396.

[197] CROSS, Frank B. **When Environmental Regulations Kill: The Role of Health/Health Analysis**, Ecology Law Quartely, Nº 22, 1995. Disponível em: http://scholarship.law.berkeley.edu/elq/vol22/iss4/2.

uma apreciação compreensiva dos riscos para incluir na avaliação também aqueles decorrentes da própria regulação.

Posição similar é a defendida por Indur Goklany[198], para quem a maioria das formulações do princípio da precaução não fornece parâmetros para a avaliação de políticas que possam gerar não só danos, mas também ganhos incertos. Para ele, o princípio da precaução leva os créditos pela redução de potenciais riscos à saúde e ao meio ambiente que decorrem das medidas restritivas, mas ignora qualquer responsabilidade pelo aumento ou prolongação de riscos causados por elas causados, pelo que ele defende um modelo de aplicação do princípio da precaução que inclua a análise risco/risco e permita a comparação dos diversos riscos em relação à sua natureza, severidade, magnitude, imediatidade, irreversibilidade e outras características.

Vale notar que tais críticas não atingem o âmago do princípio da aplicação, mas antes podem ser consideradas como uma reformulação do princípio, que seria expandido e passaria a incorporar um melhor reconhecimento da totalidade das consequências da ação reguladora.

Mais contundente é a posição de Cass Sunstein[199], para quem o princípio da precaução não pode ser aceito como uma espécie de seguro regulatório contra os riscos, posto que os riscos estão presentes em todas as atividades humanas e até mesmo na inação. Ele sustenta que o maior problema do princípio da precaução não é sua indefinição conceitual ou a desconsideração pelo custo das medidas precautórias, mas sim o fato de que ele não oferece qualquer parâmetro para a tomada de decisão e, portanto, não tem utilidade na análise de riscos. Segundo o autor, em suas versões fracas, o princípio da precaução é um truísmo que somente serve para afastar os discursos interessados na manipulação da opinião pública, como os que afirmam ser ilegítima a regulação restritiva quando não houver certeza acerca do possível dano, o que, se admitido, impediria qualquer regulação em contextos de incerteza. Assim, para o autor, as versões fracas do princípio da precaução devem ser tidas como corretas, podendo ser aceitas como incontroversas e até banais, mas não fornecem nenhum parâmetro sobre como deve o governo responder aos riscos.

Por outro lado, ainda segundo Sunstein, as versões mais fortes do princípio tampouco teriam utilidade, dado que não oferecem parâmetros para a tomada de decisão nos casos em que a tecnologia ou a atividade a ser regulada gere simultaneamente riscos e benefícios. Em

---

[198] GOKLANY, Indur. **Precaution without perversity: a comprehensive application of the precautionary principle to genetically modified crops**. Biotechnology Law report, Vol. I, n. 3, 2001.

[199] SUNSTEIN, Cass. **Laws of fear: beyond precautionary principle.** Cambridge: Cambridge University Press, 2005, p. 26-34

sua formulação forte, o princípio da precaução seria paralisante, pois proíbe a ação, a inação, e tudo o que estiver entre uma coisa e outra.

Assim, segundo Sunstein[200], nenhuma das versões do princípio da precaução fornece parâmetros que sirvam de guia sobre como devem as autoridades responsáveis pela regulação responder aos riscos e ameaças complexos com que se deparam. O princípio da precaução, assim, seria uma forma cruel e às vezes perversa de promover os objetivos de proteger a sociedade contra riscos.

A solução, segundo Sunstein, seria a elaboração de uma nova forma de tratamento do risco, sob a forma de um conjunto de princípios que formam um modelo específico de análise custo-benefício, baseado numa abordagem que ele chamou de liberalismo paternalista, que poderia fornecer parâmetros coerentes para a o balizamento de tomada de decisões pelo poder público numa sociedade democrática em face do medo da população. Esse conjunto de princípios, por ele denominado *laws of fear*, operaria nos casos de riscos danos catastróficos, de danos irreversíveis e de danos significativos para os quais seja necessária a construção de uma margem de segurança.

Na realidade, entretanto, verifica-se que a proposta de Sunstein pode ser tida como uma espécie de reformulação da análise de risco que, em última análise, pode ser compreendida como uma das formulações da versão fraca do princípio da precaução, na medida em que parametriza as medidas a serem levadas em conta para que os potenciais riscos sejam minorados.

Entendemos, portanto, que no contexto das novas tecnologias, onde não é aconselhável (na verdade, provavelmente sequer seria possível) a adoção de um marco regulatório paralisante, somente as versões mais fracas do princípio da precaução podem ser utilizados, de modo a possibilitar a intervenção estatal mesmo diante da inexistência de certeza quanto aos eventuais danos (adoção da concepção da precaução como não exclusão) ou mesmo, em situações específicas, como a dos veículos autônomos, por exemplo, para possibilitar que sejam impostas condutas, procedimentos e protocolos a serem seguidos para garantir que o funcionamento da internet e do ambiente digital do ciberespaço dê dentro de uma margem mínima de segurança no que diz respeito à tutela dos direitos fundamentais, inclusive o da privacidade (adoção da concepção da precaução como margem de segurança).

[200] IDEM, IBIDEM. p. 24

Nesse sentido é a visão de Bioni e Maria[201], para quem o princípio da precaução aplicado às novas tecnologias deve se ater a dois vetores: a abertura do debate regulatório, de modo que todos os atores envolvidos nas escolhas que a implementação das novas tecnologias impõem, desde aqueles que as desenvolvem até aqueles sobre os quais recairão seus efeitos, possam participar ativamente das definições sobre a distribuição dos riscos e a implementação de medidas regulatórias voltadas à redução das incertezas quanto aos riscos e benefícios, de modo que as decisões possam ser tomadas a partir de um contexto de menor assimetria informacional. Como afirmam os autores,

> Nesse sentido, leis gerais de proteção de dados pessoais, leis setoriais de dados biométricos e de reconhecimento facial apresentam um ferramental precaucionário a ser analisado. A sua calibração variará a escala em baixa, moderada e alta quanto ao nível de prudência acerca do emprego de IA. Ao contrário de paralisia ou inação, a execução de relatórios de impacto à proteção de dados pessoais, de mecanismos de auditoria e conversas com os órgãos reguladores e outros atores afetados são ações que podem servir de força motriz consciente e responsável para o lançamento dessa tecnologia no meio ambiente (Abramovay, 2016).

O princípio da precaução, assim, constitui uma importante força motriz da atividade regulatória das novas tecnologias, informando e conformando a atuação dos agentes reguladores. O regime de proteção de dados na legislação tem sido fortemente influenciado pela precaução, o que é certamente uma decorrência desse clima próprio da sociedade de risco. A difusão de uma sensação generalizada de medo e ansiedade quanto aos riscos e incertezas influencia tanto os costumes quanto as práticas de mercado e a tecnologia, por isso que a atividade regulatória é fortemente influenciada pelo princípio da precaução.

Nesse ponto, cabe ressaltar que a busca por segurança e a tentativa de se gerenciar riscos futuros por meio de lei e normas administrativas abre margem para uma discussão acerca do objetivo da própria atividade regulatória, que passam a ser buscados fora do mercado. Por isso, cabe aqui tratar da regulação da internet e das novas tecnologias de informação e comunicação como forma de tutelar o interesse público.

[201] BIONI, Bruno e MARIA, Luciano. **O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o Seu Portal de Entrada?** p.20

2.8 REGULAÇÃO DA INTERNET E A TUTELA DO INTERESSE PÚBLICO

Segundo o relatório “Digital 2021”, elaborado pela parceria Hootsuite/We are social, quase 60% da população mundial utiliza a internet, em um quantitativo de cerca de 4,66 bilhões de pessoas[202]. No Brasil, segundo pesquisa realizada pelo Comitê Gestor da Internet no Brasil (CGI.Br), em 2020 (,) 83% dos domicílios tinham acesso à internet. Cerca de 152 milhões de brasileiros eram usuários, o que representa 81% da população com dez anos ou mais.[203]

O imenso volume de dados produzido diuturnamente em nossa sociedade torna necessário que os riscos inerentes a essa nova forma de organização social sejam adequadamente tratados, já que é preciso reconhecer que a proteção à intimidade deve ser compatibilizada com a tutela de outros interesses públicos relevantes, como a prevenção e repressão a atividades criminosas, por exemplo.

De fato, é evidente que o enorme volume de dados produzido e tratado através da rede mundial de computadores representa uma importante fonte de provas para a persecução penal, sendo certo que para alguns crimes, em especial aqueles onde há necessidade de se monitorar fluxos financeiros, a obtenção de dados telemáticos (aqui incluindo o acesso ao conteúdo de e-mails e mensagens trocadas através de aplicativos) é, senão a única, pelo menos a mais efetiva forma de o Estado poder obter os elementos necessários para levar adiante uma ação penal e, assim, conseguir atingir os objetivos de repressão e prevenção (geral e específica) de atividades criminosas. Ademais, para crimes de especial gravidade, o recurso aos dados e informações existentes na internet pode representar a melhor forma de tutela de direitos fundamentais das vítimas (pensemos nos crimes de tráfico de pessoas ou extorsão mediante sequestro, por exemplo).

A constatação da efetividade que tais recursos podem emprestar à persecução penal demonstra que, na verdade, a tutela da privacidade dos indivíduos no ciberespaço sofre ameaças de duas ordens distintas.

A primeira das “ameaças” à privacidade é a que se apresenta de forma mais ostensiva, já que é aquela decorrente da atuação das empresas de tecnologia, que, no mais das vezes, sustentam na obtenção de dados pessoais de seus usuários o seu modelo de negócio. Gigantes como a Alphabet (controladora do Google), Meta (controladora do Facebook), Amazon e

---

[202] **Digital 2021. Global overview report**. Disponível em https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/

[203] COMITÊ GESTOR DA INTERNET BRASIL. Resumo Executivo TIC Domicílios 2020. disponível em https://cetic.br/media/docs/publicacoes/2/20211124201505/resumo_executivo_tic_domicilios_2020.pdf

Apple, por exemplo, obtêm suas receitas da comercialização dos dados pessoais de seus usuários para os interessados em propaganda dirigida e contextual, pelo que coletam diariamente uma enorme quantidade de dados que são armazenados e tratados em datacenters espalhados ao redor do mundo.

A ameaça que as novas tecnologias da informação em geral (e a internet em particular) representam à privacidade dos cidadãos e a necessidade de se limitar o poder das empresas de tecnologia, adequando suas práticas a um marco legal que possibilite a concorrência, a entrada de novas empresas, a proteção do consumidor e, principalmente, que o cidadão tenha controle sobre o acesso e o conteúdo dos dados que ele disponibiliza, é uma dos temas mais constantes nas discussões acadêmicas sobre a regulação das novas tecnologias[204], tendo também se firmado como uma das preocupações centrais dos legisladores e reguladores, do que o Regulamento Geral sobre a Proteção de Dados (EU 2016/679), a Lei Geral de proteção de dados pessoais recentemente aprovada no Brasil (Lei 13.709/2018) e diversos diplomas legais aprovados nos Estados Unidos são exemplos[205].

Há, porém, uma outra fonte de riscos à privacidade digital que tem recebido consideravelmente menos atenção: aquela decorrente da utilização, pelos Estado, das novas tecnologias de informação e comunicação como fonte de obtenção dos elementos de que os órgãos governamentais necessitam para sua atuação, o que é especialmente sensível no campo criminal.

De fato, a proteção de dados pessoais, no que diz respeito à atuação estatal ligada às atividades de prevenção, detecção, repressão e punição de infrações penais, consiste em um campo que, especialmente no Brasil, tem passado ao largo das discussões acerca da regulação da internet, mesmo a despeito de esta forma de atuação estar se tornando cada vez mais essencial para a persecução penal.

Essas duas ordens de risco à privacidade representam desafios à regulação da internet e das novas tecnologias, pois colocam em xeque a visão da internet como "terra sem lei" ou de espaço de liberdade sobre o qual não poderia haver intervenção regulatória. Entretanto, dada a importância que a vida no ciberespaço assumiu na sociedade contemporânea, já não há

---

[204] Sobre o tem, entre outros, ver RODOTÀ, Stefano. **A vida na sociedade da vigilância - a privacidade hoje.** Rio de Janeiro: Renovar, 2008. Tradução de: Danilo Doneda, Luciana Cabral Doneda

[205] V.g. Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); the Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); the Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); the Data Breach Notification Act, S. 1408, 112th Cong. (2011); the Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011); the Secure and Fortify Electronic Data Act of 2011, H.R. 2577, 112th Cong. (2011); and the Cybersecurity Enhancement Act of 2011, H.R. 2096, 112th Cong. (2011)

mais espaço para se sustentar que a internet não pode ser regulada. O compromisso que o estado deve ter com a tutela de direitos fundamentais lhe impõe o dever de atuar ativamente na garantia de que em todos os setores da vida social esses direitos serão respeitados pelo Estado, protegidos contra eventuais violações por parte de terceiros, e promovidos no meio social para que sejam constantemente difundidos e tenham seu valor reconhecido e respeitado por todos.

Por isso, a ideia de que o ciberespaço não pode ser regulado pelo Estado não pode ser aceita, já que, dentro ou fora da internet, a construção de um mundo onde a liberdade possa florescer depende da existência de possibilidade do exercício de controle legítimo, a ser exercido de forma proporcional e com vistas à tutela de direitos fundamentais.

A questão que se coloca, assim, é a de saber como esse controle deve ser feito, ou seja, como deve ser exercida a função regulatória para que os interesses públicos, com especial menção àqueles relacionados ao exercício dos direitos e liberdades fundamentais, possam ser atendidos.

Neste ponto, deve ser salientado que as teorias regulatórias do interesse público, que atribuem aos agentes reguladores o desejo de alcançar objetivos coletivos e promover o bem estar geral da coletividade, apresentam como evidentes pontos fracos a indefinição do conceito de interesse público e uma certa dose de crença benevolente no desinteresse e isenção dos reguladores.

De fato, a definição do que é interesse público, especialmente numa sociedade complexa e pluralista, tende a ser uma questão extremamente complexa, cuja solução costuma apontar para a definição pelos fóruns de deliberação política, como o Parlamento. Por isso, alguns teóricos do interesse público, sustentam que o interesse público a ser buscado pela regulação é aquele decorrente da eficiência econômica, cabendo à regulação unicamente a tarefa de corrigir as falhas de mercado, já que

> Qualquer tentativa de formular uma lista abrangente de objetivos de interesse público que possa ser usada para justificar a regulamentação seria fútil, uma vez que o que constitui o "interesse público" irá variar de acordo com o tempo, lugar e os valores específicos mantidos por uma determinada sociedade.[206]

[206] CF. MORGAN, Bronwen e YEUNG, Karen. **An Introduction to Law and Regulation: Text and Materials.** Cambridge: Cambridge University Press, 2007. p. 14. Tradução nossa. No original: “Any atempt to formulate a comprehensive list os public interest goals wich may be used to justify regulation would be futile, since what constitutes the ‘public interest’ Will vary according to time, place, and the specific values held by a particular society.”

Entretanto, como demonstrou Prosser[207], a busca pela eficiência econômica e correção das falhas de mercado não devem ser os únicos motivos para justificar a regulação, que também tem um importante papel na criação dos mercados, na proteção de direitos humanos e na implementação de solidariedade social.

A dificuldade inerente à falta de definição pode ser superada através da utilização de um modelo procedimental de regulação que, vendo regulação como um sub-ramo do governo, se volta à Constituição[208]. Essa abordagem traria duas vantagens: ajudaria a estabelecer uma base substantiva para o conceito de interesse público a ser buscado pelo regulador, ancorado na Constituição e, além disso, serviria de parâmetro para as ponderações entre valores conflitantes que devem ser regulados.

Ressalte-se que a utilidade dessa construção é evidente mesmo em se tratando de uma constituição analítica, como a brasileira de 1988, dado que, mesmo a despeito de um texto constitucional amplo não ser suficiente para, por si, deixar claro todos os objetivos a serem perseguidos, podem desde logo afastar algumas abordagens claramente contrárias ao texto constitucional.

Cabe notar, ainda, que a essa ancoragem constitucional, ainda muito ampla e no mais das vezes incapaz de possibilitar concretamente a definição das políticas a serem adotadas, deve ser agregada a necessidade de que procedimentos que assegurem a participação dos interessados sejam adotados para que efetivamente a regulação possa servir ao interesse público.

Por outro lado, cabe referir que a adoção de um conceito amplo de regulação possibilita incorporar aos modelos e análises as forças não estatais que atuam na conformação de comportamentos, mas também permite visualizar de modo mais claro a intersecção entre as atividades estatais tipicamente administrativas, usualmente identificadas como regulatórias, e aquelas que, apesar de também serem destinadas a obter uma alteração de comportamento de terceiros, tradicionalmente são vistas como algo completamente distinto de regulação, como o direito tributário e o direito civil, por exemplo. Nessa perspectiva, também o direito penal e o direito processual penal, instrumentos por excelência da tutela de direitos fundamentais e meios de implementação dos limites da política criminal, devem ser compreendidos como fontes de regulação.

---

[207] PROSSER, Tony. **Two visions of regulation.** Paper by Tony Prosser for 'Regulation in the Age of Crisis', University College. Dublin, 2010. Disponível em http://regulation.upf.edu/dublin-10-papers/1H1.pdf

[208] CF. PROSSER, Tony. Op. Cit.

É que, como já assinalado, o Direito, como uma ciência essencialmente prática, voltada à solução de problemas concretos, não pode ser visto de maneira estanque e fragmentada, como se a forma de regulamentação de um dos ramos fosse algo totalmente indiferente aos demais. Na verdade, não é possível se pensar validamente na busca por soluções em uma dada área sem levar em consideração as repercussões decorrentes da disciplina dos outros ramos do direito sobre aquele objeto. Não é por outra razão que no âmbito do direito penal, por exemplo, o exercício regular de direito e o estrito cumprimento de dever legal excluem a antijuridicidade de uma conduta típica, descaracterizado a ocorrência de um crime (art. 23, III do Código Penal), da mesma forma que o exercício regular de direito também exclui a ocorrência de um ilícito civil (art. 188, I do Código Civil).

Essa concepção ampla é imprescindível quando o que se busca é compreender de que forma as forças regulatórias atuam sobre um dado objeto. Aqui, uma vez que o objeto do presente estudo é a forma como a regulação da internet pode ser compreendida como instrumento de tutela de direitos fundamentais em matéria penal, a adoção de uma perspectiva ampla da atividade regulatória é pressuposto essencial para a compreensão dessa interação entre regulação da internet e persecução penal.

Entretanto, esta é ainda uma abordagem incompleta do fenômeno, uma vez que não basta identificar as forças que atuam visando a modificar as respostas e comportamentos, sendo necessário que também o objeto da regulação seja adequadamente compreendido, por isso que se faz necessária uma incursão acerca da privacidade, de modo a possibilitar a posterior compreensão da relação entre surveillance e direito penal.

3. A PRIVACIDADE

> *"Uma existência vivida inteiramente em público, na presença de outros, torna-se, como diríamos, superficial. Retém a sua visibilidade, mas perde a qualidade resultante de vir à tona a partir de um terreno mais sombrio, terreno este que deve permanecer oculto a fim de não perder sua profundidade num sentido muito real e não subjetivo" (Hannah Arendt).*
>
> *A civilização é o progresso em direção a uma sociedade de privacidade. (Ayn Rand)*

A ampla disseminação das novas tecnologias de comunicação e informação, que tornaram corriqueiras as ações de coleta, armazenamento, análise e processamento de quantidades enormes de dados pessoais dos indivíduos, é uma das razões pela qual a privacidade parece estar cada vez mais em rota de colisão com a tecnologia[209].

Desde a sua primeira formulação teórica, que remonta a um artigo de Samuel Warren e Louis Brandeis publicado em 1890[210], o direito à privacidade, então concebido como o direito de ser "deixado em paz", teve sua evolução intimamente ligada às mudanças tecnológicas da era industrial. Brandeis e Warren escreveram motivados pela busca de garantir proteção legal contra o uso de máquinas fotográficas portáteis e a publicação de fofocas em jornais impressos, sustentando que a proteção à privacidade por meio da responsabilização civil seria uma mostra de como o Direito deveria evoluir para responder às mudanças nas circunstâncias sociais.

A cada desenvolvimento de uma nova tecnologia relacionada à comunicação e informação, segue-se uma onda de temor pelo fim da privacidade, principalmente por parte daqueles que veem nas mudanças uma espécie de subversão disruptiva da ordem social. Não é por outra razão que o historiador Lawrence Friedman[211] afirma que essas reações em grande medida refletem um sentimento de ansiedade das elites, gerado pelo medo de que sua

---

[209] CF. STALLA-BOURDILLON, Sophie; PHILLIPS, Joshua e RYAN, Mark D. **Privacy vs. Security**, 2015.

[210] WARREN, Samuel D. e BRANDEIS, Louis D. **The Right to Privacy**. 1890. Disponível em https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[211] RICHARDS, Neil M. **Four Privacy Myths.** in SARAT, Austin (org). **A world without privacy : what law can and should do?** 2015, pp. 33-82

exposição pelas novas ferramentas tecnológicas possa de alguma forma ameaçar sua posição de dominância.

O medo de que as novas tecnologias acarretem o fim da privacidade, portanto, não é algo novo, nem específico da era da internet, como bem demonstra o contexto em que foi criada a doutrina da proteção legal da privacidade no final do século XIX. Na verdade, a questão está sempre ligada a uma nova forma de utilização da informação, que subverte as regras anteriores. Reações similares também ocorreram com o início da utilização extensiva dos computadores, nos anos 1980, com o início da utilização da internet comercial em larga escala, nos anos 1990, com a explosão de celulares nos anos 2000, com a popularização das redes sociais em 2010, e certamente é o que ocorrerá também com o *big data*, com a inteligência artificial, a disseminação da internet das coisas e com todas as evoluções futuras da forma como lidamos com a informação.

De fato, a correta análise dos problemas sociais ligados à sociedade e à utilização das novas tecnologias pressupõe uma abordagem mais ampla, que permita superar a visão da tecnologia que se limita ao construto, isto é, ao produto ou serviço tecnológico oferecido ou colocado à disposição, mas que compreenda toda a ampla variedade de práticas organizacionais e sociais associadas à tecnologia.

As análises das novas tecnologias devem transcender a própria tecnologia e buscar compreender de que forma ela afeta as relações sociais, tanto na esfera pública quanto na individual, tornando-se profundamente imbricada na vida das pessoas e organizações, afetando seu modo de ser, pensar e agir. Isso é especialmente importante quando pensamos nas novas tecnologias de informação e comunicação, em especial a internet, que tem como característica marcante sua ubiquidade e crescente onipresença, que foi muito ampliada com a popularização da utilização de aparelhos móveis de telefonia como forma de acesso e que, com a progressiva difusão da internet das coisas, tende a se tornar ainda mais presente.

Uma das mais importantes questões que a tecnologia digital introduz é como lidar com o armazenamento das informações. Computadores analógicos eram máquinas de cálculo que não geravam dados sobre seu uso, a não ser que fossem construídos dispositivos para esta finalidade específica. As modernas tecnologias de informação e comunicação, entretanto, a todo momento estão não só gerando informações sobre sua utilização, mas também compartilham essa informação com outros sistemas conectados à internet e, assim, retroalimentam-se e formam uma imensa teia de aparatos de controle e vigilância.

Assim, não resta dúvida de que a privacidade nos tempos que correm passa por profundas transformações, tornando necessária a discussão de seus contornos em um mundo

cada vez mais interconectado e imerso em uma cultura digital, para que possamos compreender seu valor e o peso relativo que a ela deve ser conferida nas colisões com outros valores.

A necessidade de se reconfigurar os contornos da privacidade é ainda maior no campo penal, ante a constante utilização de aparatos de vigilância para fins de policiamento e segurança pública. Nessa seara há uma espécie de diminuição geral do valor conferido à privacidade, que comumente é colocada em segundo plano em nome da busca por efetividade da prevenção ou repressão de crimes, o que não ocorre com tanta intensidade em outras áreas, especialmente no campo das relações privadas.

De fato, em contextos diferentes daqueles relativos à segurança pública ou nacional, a ideia de que a privacidade é um valor essencial, devendo ser respeitada, protegida e promovida por todos, é amplamente difundida e aceita. Aliás, talvez seja exatamente em decorrência desse amplo reconhecimento no campo das relações privadas que, frequentemente, a privacidade é pensada unicamente sob esse ângulo.

Nesse sentido, o artigo XII da Declaração Universal dos Direitos Humanos, adotada em 1948 pelas Nações Unidas e atualmente subscrita por todos os seus 193 países-membros, proclama que "ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques."[212]. No mesmo sentido, a Convenção Interamericana dos Direitos Humanos dispõe em seu art. 11 que:

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.

2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.

3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Entretanto, a privacidade não pode ser reduzida a este aspecto relacionado a relações privadas e individuais. Na verdade, longe de se tratar unicamente de um mero refúgio de intimidade para o indivíduo, de uma zona de conforto e proteção contra a intromissão

[212] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Disponível em https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf

indevida de outras pessoas em assuntos íntimos (elementos que, ressalte-se, por si só seriam de extrema importância), a privacidade também diz respeito a outros aspectos essenciais da vida, ligados à proteção do indivíduo contra o abuso do poder, por parte de agentes estatais, por parte de detentores do poder econômico, ou, ainda, por parte de uma coletividade qualquer que ocasionalmente esteja em posição de exercer poder sobre o indivíduo.

Há, portanto, uma enorme variedade de questões que envolvem a proteção à privacidade. Questões tão diversas quanto a divulgação de fatos inverídicos sobre uma pessoa, a discussão acerca da possibilidade de utilização de dados obtidos no celular de um preso em flagrante ou os limites do exercício de direitos reprodutivos pelas mulheres estão diretamente ligadas à noção da privacidade.

Não há uma definição sobre o conceito de privacidade que possa ser universalmente aceita. Na verdade, tal como "liberdade" ou "igualdade", "privacidade" é uma daquelas palavras utilizadas cotidianamente sobre as quais todos têm uma noção, mas ninguém consegue definir ao certo. Isso é especialmente verdadeiro no uso cotidiano da expressão, onde no mais das vezes ela é utilizada como sinônimo de intimidade.

A multiplicidade de situações em que a privacidade se apresenta, bem como o fato de que o contexto e as razões pelas quais ela é discutida variam muito de acordo com a realidade sócio-histórica, estão certamente entre as causas do enorme desafio de se estabelecer uma definição precisa de seu conceito.

Mesmo quando nos afastamos do senso comum e adentramos no campo da Ciência, tampouco é possível achar uma definição unívoca e consensualmente aceita de privacidade. Aliás, como afirma Kasper[213], a notória dificuldade de se estabelecer o significado deste termo tão amplamente utilizado é bem demonstrada pelo fato de a grande maioria dos estudos sobre o tema iniciar com uma introdução tratando exatamente dessa dificuldade conceitual.

Inexiste consenso mínimo entre juristas, filósofos, cientistas sociais, engenheiros ou cientistas da computação acerca do que pode ser caracterizado como privacidade. Por essa razão Daniel Solove[214] afirma que a privacidade é "um conceito em desordem. Ninguém consegue articular o que ela significa", e Wadrow Hartzog[215] a qualifica como um conceito

---

[213] KASPAR, Debbie, **The Evolution (or Devolution) of Privacy**, Sociological Forum, n. 20, 2005, p. 72. Disponível em http://www.jstor.org/stable/4540882

[214] Tradução nossa. No original: **"**a concept in disarray. Nobody can articulate what it means". SOLOVE, Daniel. **Understanding privacy.** Cambridge: Harvard University Pres, 2008. Disponível em http://ssrn.com/abstract=1127888.

[215] HARTZOG, Woodrow. **Privacy´s blueprint. The battle to control the design of new Technologies**. Cambridge: Harvard University Prees, 2018. P. 10

amorfo e elusivo. Para Cancelier[216], a privacidade pode ser adjetivada como elástica, flexível e fluida. Alan Westin afirmou que "poucos valores tão fundamentais para a sociedade foram deixados tão indefinidos pela teoria social"[217] e Mendes e Branco[218] afirmam que "não obstante a relevância do tema, verificam-se hesitações quando se trata de definir o que seja exatamente o direito à privacidade". Após realçar que a privacidade é objeto de estudo de áreas que vão desde a filosofia até a Ciência Política, passando pela Ciência da Computação, Engenharia, Comunicação, Ciência da Informação e Direito, Helen Nissenbaum[219] afirma que o único ponto sobre o qual há uma quase unanimidade é que a privacidade é um objeto complexo e confuso.

A privacidade é um conceito vago e de contornos extremamente nebulosos, o que talvez seja uma decorrência do fato de que ela está ligada a situações que vão desde a proteção à liberdade de pensamento até a proteção contra intervenções excessivas do Estado sobre o indivíduo, passando, entre outros aspectos, pela proteção à honra e à imagem, pela proteção ao domicílio, pelo controle sobre o próprio corpo, pelo direito de ser deixado em paz, pela proteção ao sigilo de comunicações e de dados, bem como pela limitação do poder estatal de vigilância e de persecução penal.

Outro aspecto que contribui muito para a dificuldade conceitual são as mais diversas respostas que as diferentes sociedades apresentam para as questões relacionadas à privacidade, tornando ainda mais árduo se estabelecer um conceito único que abarque todas a variedade de questões relacionadas à privacidade. Entretanto, como afirma Kaspar[220], apesar das convenções sociais em torno do que significa privacidade variarem muito de acordo com o contexto sócio-histórico, as pesquisas antropológicas demonstram que, mesmo quando se leva em consideração aquelas sociedades em que havia menos espaço para os indivíduos se manterem longe do grupo, o desejo por privacidade sempre foi algo comum, presente em todas as sociedades[221].

---

[216] CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro.** Sequência, n. 76, p. 225. Disponível em

[217] Tradução nossa. No original: "few values so fundamental to society as privacy have been left so indefined in social theory". Citado em SOLOVE, Daniel. **Conceptualizing privacy.** California Law Review, vol. 90. 2002**. P.** 1089

[218] MENDES, Gilmar Ferreira e BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 8ª. Ed. São Paulo: Saraiva, 2013, p. 281.

[219] NISSENBAUM, Helen. **Privacy in context. Technology, policy and the integrity of social life** Stanford Law Books: Stanford, 2010. P. 67

[220] KASPAR, Debbie. **The Evolution (or Devolution) of Privacy**, Sociological Forum, n. 20, 2005, p. 69. Disponível em http://www.jstor.org/stable/4540882

[221] Danilo Doneda parece discordar dessa ideia, quando afirma que "não havia lugar para a tutela jurídica da privacidade em sociedades que conferiam a sua regulação a outros mecanismos". Entretanto, acreditamos que

Na verdade, a maioria das tentativas de se estabelecer um conceito unívoco de privacidade acaba resultando ou na formulação de um conceito genérico demais, a ponto de perder utilidade, já que pode ser aplicado a toda e qualquer situação, ou estreito demais, deixando de fora aspectos essenciais frequentemente relacionados à noção de privacidade.

A despeito de toda essa dificuldade conceitual, legisladores, reguladores e operadores do direito são constantemente confrontados com questões que dizem respeito, direta ou indiretamente, à privacidade. Especialmente quando se discute sobre como agir diante de uma situação em que a privacidade se apresenta em colisão com outros direitos fundamentais, como quando a honra é contraposta à liberdade de expressão, ou quando o sigilo de dados é confrontado com a necessidade de proteção à segurança pública, a compreensão do que seja a privacidade, de quais são seus contornos e qual a importância de sua proteção, assumem uma especial importância, pois sua ausência faz com que a proteção à privacidade quase sempre seja relegada a um plano secundário[222].

Assim, do ponto da formulação de políticas públicas, a definição dos contornos da privacidade é absolutamente necessária, a fim de possibilitar que a avaliação de custo e benefício das medidas regulatórias a serem adotadas possa ser feita a partir de análises de contextos e circunstâncias concretas. Na realidade, falta de compreensão do que é a privacidade e de qual sua importância fazem com que muitas vezes somente os valores a ela contrapostos sejam percebidos como dignos de proteção, levando o legislador e as autoridades regulatórias a menosprezarem o que está em risco quando a privacidade está sob ameaça e ignorarem o papel que a lei e a regulação deveriam assumir na proteção da privacidade.

Por outro lado, a necessidade de se compreender e valorar adequadamente a privacidade é também extremamente importante no campo jurisdicional, quando se trata de aplicar o direito para solucionar problemas relacionados à privacidade, já que ela é vista como um princípio e, atualmente, é quase unânime o entendimento de que a concretização de princípios deve ser feita através por meio da técnica da ponderação e do sopesamento, e não da mera subsunção[223].

---

a divergência aqui é mais aparente do que real, posto que possivelmente o autor neste trecho não se referia à ideia de privacidade, mas à sua tutela jurídica, ao direito à privacidade, o que fica evidente quando afirma em seguida que "o despertar do direito para a privacidade ocorreu justamente num período em que muda a percepção da pessoa humana pelo ordenamento e ao qual se seguiu a juridificação de vários aspectos do cotidiano". Ver DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006, p. 08.

[222] Cf. SOLOVE, Daniel. **Nothing to hide. The false tradeoff between privacy and security.** New Haven: Yale University Press, 2011**.**

[223] A definição de princípios (aplicáveis por ponderação) em contraposição a regras (aplicaveis por subsunção) é fonte de infindáveis divergências doutrinárias, havendo mesmo quem afirme inexistir qualquer

Em um processo judicial, a concretização de um princípio tem como primeiro passo a realização de uma operação de valoração deste princípio, de modo a estabelecer não só sua posição prévia (isto é, qual o seu grau de importância abstrato quando comparado com outros princípios), mas principalmente para poder estabelecer concretamente qual o grau de interferência admissível quando de uma colisão com outro princípio, tal como a liberdade de expressão ou a segurança pública. Por isso é que não só na formulação de políticas públicas, mas também na aplicação judicial do Direito, é preciso que a privacidade e seu valor sejam corretamente identificados.

Nessas condições, sem a compreensão do conceito de privacidade, tanto a regulação quanto a solução judicial dos problemas a ela relacionados perdem em racionalidade, favorecendo a adoção de soluções voluntaristas e com poucas condições de efetivamente possibilitar que se alcance o equilíbrio dos interesses colidentes. Por isso que, mesmo a despeito das dificuldades, é necessário buscar-se no mínimo elementos que permitam compreender corretamente a privacidade.

Para tanto, é importante que façamos uma incursão sobre a evolução da própria ideia da privacidade, sobre as concepções filosóficas que lhe dão suporte e sobre as diferentes valorações do público e do privado, na certeza de que, como afirmou o historiador Marc Bloch, "nos antípodas dos exploradores de origens, situam-se os devotos do imediato".

3.1. PÚBLICO E PRIVADO: CONECTANDO A PRIVACIDADE COM A LIBERDADE, A IGUALDADE E A DEMOCRACIA

De acordo com sua noção atualmente mais difundida, a ideia de privacidade mantém uma ligação estreita com a ideia de liberdade. Não é por acaso que são recorrentes as distopias de um futuro em que um déspota autoritário se mantém no poder eliminando a privacidade e controlando todos os aspectos das vidas da população, acabando com a liberdade individual.

---

diferença ontológica entre tais categorias normativas. Entretanto, pode-se afirmar que a posição mais usualmente adotada pelo Judiciário no Brasil é a de Robert Alexy, que caracteriza princípios (categoria na qual se incluiria a privacidade) como um mandamento de otimização, isto é, como uma ordem para que algo seja realizado na maior medida possível, de acordo com as condições fáticas (apreciadas nas categorias da adequação e da necessidade) e jurídicas (quando entram em jogo os princípios contrapostos). Os princípios, assim, diversamente das regras (que são aplicadas segundo a lógica do tudo-ou-nada), têm uma dimensão de peso e precedência, podendo ser cumpridos em maior ou menor grau, de acordo com as circunstâncias fáticas e jurídicas. Sobre o tema, ver ALEXY, Robert. **Teoria dos direitos fundamentais.** São Paulo: Malheiros, 2008.

Sejam as teletelas da Oceania de George Orwell, seja o olho de Sauron na Mordor de Tolkien, a existência de instrumentos de vigilância e controle dos indivíduos têm sido a forma preferencial pela qual a ficção retrata a atuação do totalitarismo. A redução do espaço privado quase sempre aparece como um pressuposto para o exercício e para a manutenção do poder nas ficções totalitárias, onde a conquista da liberdade é representada pela busca de um espaço próprio e particular no qual o indivíduo possa exercer livremente sua subjetividade, sem a vigilância e o controle do poder opressor.

A privacidade, nessa perspectiva, constitui um contraponto necessário à ideia de um espaço público de visibilidade no qual o indivíduo não consegue ser totalmente livre. A garantia da manutenção de um espaço privado, protegido contra a vigilância e o controle pelos poderes políticos e econômicos, é vista como condição para que cada um possa ser e pensar de forma autônoma.

A separação entre o espaço público e o privado e a preocupação com a privacidade como elemento da liberdade, todavia, não é produto da modernidade e nem mesmo algo novo. De fato, no Código de Hamurabi e no Direito Romano já havia previsões legais protegendo a casa contra intrusos[224].

A valorização do espaço privado em sua contraposição ao público e ao governamental, entretanto, é algo que mudou muito ao longo do tempo, já que historicamente nem sempre a esfera privada foi tida como um espaço a ser protegido, o que fica evidente quando se analisa a evolução de tais conceitos. Como afirma Habermas[225], público e privado são categorias tradicionais cujo sentido foi sendo construído ao longo de períodos históricos diversos e que têm origem grega, mas que nos foram transmitidas a partir de seu molde romano.

Na Grécia antiga, havia uma distinção clara entre a esfera privada, constituída pela esfera da casa (*oikos*), ligada à família, àquilo que é próprio ao homem e que se fundava nas relações como a *phratria* (irmandade) e a *phyle* (amizade)[226], e o espaço público, a *Pólis*, domínio da vida política, da qual os cidadãos participavam através da ação (*práxis*) e do discurso (*lexis*)[227].

---

[224] CF. SOLOVE, Daniel. **Nothing to hide. The false tradeoff between privacy and security.** New Haven: Yale University Press, 2011

[225] HABERMAS, Jürgen. **Mudança estrutural da esfera pública: investigações sobre uma categoria da sociedade burguesa**. São Paulo: Editora Unesp, 2014. p. 96.

[226] CF. ANTUNES, Marco António. **O público e o privado em Hannah Arendt.** Biblioteca On Line de Ciências da Comunicação, 2004. **Disponível em http://www.bocc.ubi.pt/pag/antunes-marco-publico-privado.pdf**

[227] ARENDT, Hannah. **A condição humana.** 10ª. Ed. Rio de Janeiro: Forense Universitária, 2007. P. 34

Nas cidades-estado gregas, a esfera da *Pólis* era estritamente separada da esfera da *Oikos*. A vida pública, comum a todos os cidadãos livres, se constituía no discurso (*lexis)*, que também podia assumir a forma de deliberação de um tribunal, ou na busca da ação comum, (*práxis*) e dependia da autonomia privada do cidadão como senhor de sua casa. A esfera privada, por seu turno, mais do que ligada ao nome da casa, também estava ligada ao poder de disposição sobre a economia doméstica e sobre a família.

A noção aristotélica do homem como um ser essencialmente político, dotado de fala, reflete a visão da *Pólis* como sendo o ápice da construção social humana, posto que "ser político" significa ter a capacidade de utilização das palavras e da persuasão como formas de solucionar os problemas comuns, e não mais a violência, método pré-político de solução de problemas. É interessante notar que, segundo Arendt[228], ao definir o homem como um ser político (*zoon politikon*) e como um "ser vivo dotado de fala" (*zoon logon ekhon*), Aristóteles não pretendeu tratar do homem em geral ou mesmo da racionalidade do ser humano, mas apenas refletia sua visão acerca daquilo que ordinariamente ocorria na Grécia antiga, isto é, descrevia a realidade da época, posto que o homem que vivia fora da *Pólis,* como os bárbaros e os escravos, não participava de um modo de vida em que o discurso tivesse papel central na solução dos conflitos. A estrita separação entre o público e o privado, portanto, era uma realidade na sociedade grega, sendo um dos elementos constitutivos daquela sociedade.

Na esfera privada da Grécia antiga imperavam relações desiguais, pois se tratava de um espaço onde só o chefe da família exercia o poder sobre os seus subordinados (esposa, filhos e escravos), sendo que esse poder exercido na esfera "privada" não era alcançado e, portanto, limitado pelas leis ou pela justiça da *Pólis*. A esfera pública, por outro lado, se estabelecia em um contexto em que, apesar de ser excludente (uma vez que só admitia a participação do chefe de família), era caracterizado pela relação entre iguais (igualdade aqui entendida não como expressão de qualquer noção de justiça, mas unicamente no sentido de que as relações políticas eram estabelecidas sem noções de hierarquia). Essa distinção entre as relações do público e do privado ficam bem evidentes em Aristóteles[229], quando, ao tratar da virtude da Justiça, afirma que somente é possível haver justiça ou injustiça fora do ambiente doméstico, pois cometer injustiça em casa seria como cometer uma injustiça contra si próprio, por isso que, no espaço doméstico, não pode haver nada de "justo" ou "injusto" no sentido político.

---

[228] ARENDT, Hannah. **A condição humana.** p. 36

[229] ARISTÓTELES. **Ética a Nicômaco.** Tradução de Leonel Vallandro e Gerd Bornheim. Livro V, 6. 1134a 26-28**.** São Paulo: Nova Cultural, 1991.

Os limites entre o espaço público e o privado eram bem demarcados, de modo que o espaço privado era aquele onde as relações estabelecidas ficavam imunes aos assuntos públicos. A relação do chefe de família com os servos, os filhos ou a mulher, se situava em um campo pré-político, no qual não havia espaço para a persuasão como forma de solução de conflitos, mas somente a violência e a força. Havia um verdadeiro abismo entre o espaço público da *Pólis* e o espaço privado da *oikia* (a casa, espaço doméstico, economia domésticas, referente ao espaço físico em que se estabeleciam as relações) e o O*ikos* (bens existentes no espaço privado).

Havia, ainda, uma diferença de grau de evolução entre a *Oikos* e a *Pólis*, pois, para Aristóteles, a *Pólis* seria a mais perfeita e acabada comunidade criada pelos homens, enquanto a *Oikos* seria a comunidade mais primitiva[230]. A diferença que se estabelecia entre o privado e o público, entre o doméstico que era escravo e o chefe da casa que era um cidadão, entre um espaço onde imperava a hierarquia e outro onde imperava a igualdade, se refletia na noção de que havia atividades que deveriam ser desempenhadas escondidas, na privatividade do lar, e outras que eram dignas de serem desempenhadas em público.

Para os antigos, a privacidade implicava em privação, posto que o indivíduo deixava de participar inteiramente da vida pública, e passava a integrar um espaço em que vivia como um bárbaro ou um escravo, fora da valorizada posição do espaço público. Ou seja, o privado estava ligado a uma privação da atuação na arena política, a uma ausência do espaço público, local em que a virtude deveria se sobressair.

Para os gregos, era o fato de ser visto e ouvido que, em última análise, conferia realidade ao sujeito, possibilitando-lhe o estabelecimento de uma relação objetiva com os demais partícipes de um mundo comum de coisas. Como resume Arendt, "a privação da privatividade reside na ausência de outros; para estes, o homem privado não aparece, e, portanto, é como se não existisse[231]". Quem não pudesse participar da vida pública não era inteiramente humano, posto que estava privado de um aspecto essencial da existência, aquele que se desenvolvia na esfera pública da *Pólis.*

Assim, como afirma Maria de Fátima Francisco, "a esfera pública é o espaço da visibilidade, enquanto a esfera privada é o espaço do ocultamento"[232]. Uma consequência disso é que somente aquilo que está no espaço público é que era tido como relevante, ao passo

---

[230] FRANCISCO, Maria de Fátima Simões. **Aristóteles enquanto fonte das concepções de espaço público e espaço privado de Hannah Arendt.** Notandum, Ano X - N. 14, 2007. Disponível em http://www.hottopos.com/notand14/fatima.pdf, p. 40.

[231] ARENDT, Hannah. **A condição humana. 10ª. Ed.** Rio de Janeiro: Forense Universitária, 2007. P. 67

[232] IDEM IBIDEM, p. 45

que o privado é tido como o local em que ocorre aquilo que é irrelevante. Na bela imagem por ela construída, Arendt[233]afirma que até mesmo a meia luz que ilumina nossa vida privada e íntima deriva da intensa claridade que vem da esfera pública, ressaltando que "há muitas coisas que não podem suportar a luz implacável e crua da constante presença de outros no mundo público; neste, só é tolerado o que é tido como relevante, digno de ser visto ou ouvido, de sorte que o irrelevante se torna automaticamente assunto privado".

Vale notar que o conceito helênico de publicidade, estilizado a partir de uma auto interpretação feita pelos próprios gregos, associava a luz da publicidade à igualdade, na medida em que a publicidade permitia que todos os assuntos públicos (isto é, ligados ao bem comum) fossem discutidos por todos os cidadãos em pé de igualdade, levando a que os melhores pudessem se sobressair. O público, assim, passou a ser o espaço por excelência onde as virtudes poderiam ser preservadas, por ganharem reconhecimento.

O espaço privado, O*ikos*, era onde o homem atuava para suprir suas necessidades biológicas, garantindo sua sobrevivência. Hannah Arendt chama atenção para o fato de que o traço mais marcante da esfera familiar é que nela os homens eram obrigados a viver juntos em razão de suas necessidades e carências. Para ela, na esfera privada,

> A força compulsiva era a própria vida, os penates, os deuses do lar, eram, segundo Plutarco, 'os deuses que nos fazem viver e alimentar o nosso corpo'; e a vida, para sua manutenção individual e sobrevivência como vida da espécie, requer a companhia de outros. O fato de que a manutenção individual fosse a tarefa do homem e a sobrevivência da espécie fosse a tarefa da mulher no parto, eram sujeitas à mesma premência da vida. Portanto, a comunidade natural do lar decorria da necessidade: era a necessidade que reinava sobre todas as atividades exercidas no lar[234]

Essa condição gerava uma outra característica marcante da separação entre público e privado, a existência de uma barreira de separação decorrente das necessidades biológicas que caracterizavam o privado. Isso porque superar essa situação de necessidade para enveredar na vida política não só tinha como pressuposto a solução dos mais imediatos problemas relacionados ao atendimento às carências econômicas e à propriedade, mas também requeia que o cidadão tivesse aquela que constituía a mais importante virtude política, a coragem, posto que na *Pólis* o homem tinha que arriscar a própria vida, libertando-se do servilismo do

[233] IDEM, IBIDEM. P. 61

[234] ARENDT, Hannah. **A condição humana. 10ª. Ed.** Rio de Janeiro: Forense Universitária, 2007. P. 39/40.

amor à vida. Para Antunes[235], "a vida boa, que Aristóteles identificava com a acção política, significava a libertação do homem face às esferas do animal *laborans* e do *homo faber* efectivando-se através da virtude da coragem e da eudaimonia (vida boa)."

A participação no espaço público significava transcender a esfera da necessidade, das limitações humanas, para enveredar em um ambiente no qual o homem poderia deixar uma marca para a posteridade. A reclusão do espaço privado era identificada com o irrelevante e transitório, ao passo que o espaço público era destinado ao exercício das virtudes, que fariam com que a permanência na terra não passasse despercebida. Era no espaço público que o indivíduo tinha a possibilidade de se diferenciar dos demais, sobressaindo-se e, assim, alcançando a perenidade, deixando um legado que poderia ultrapassar a sua morte. A criação do espaço público como mecanismo de profusão de ideias relacionadas à virtude e ao bem comum foi uma consequência da necessidade de que o cidadão grego pudesse praticar a política e mostrar suas virtudes, para que elas não perecessem e desaparecessem com sua morte.

Assim, a esfera pública estava reservada ao desenvolvimento da individualidade do sujeito. Era através da afirmação por meio de ações e palavras que o indivíduo poderia transcender sua dimensão temporal, estabelecendo um legado para sempre marcado na memória dos homens. Para Hannah Arendt[236]:

> A excelência em si, *arete* como teriam chamado os gregos, *virtus* como teriam dito os romanos, sempre foi reservada à esfera pública, onde uma pessoa podia sobressair-se e distinguir-se das demais. Toda atividade realizada em público pode atingir uma excelência jamais igualada na intimidade; para a excelência, por definição há sempre a necessidade de presença de outros, e essa presença requer um público formal, constituído pelos pares do indivíduo; não pode ser a presença fortuita e familiar de seus iguais ou inferiores.

Vale ressaltar que é completamente incabível qualquer anacrônica tentativa de se avaliar a democracia grega a partir de valores da sociedade contemporânea, uma vez que a condição de possibilidade da democracia grega era a restrição da possibilidade de participação na esfera pública àqueles poucos que eram capazes de alcançar o sucesso em seu lar, libertando-se das amarras da necessidade econômica de prover a subsistência própria e dos seus. Por isso que, para os pouco que conseguiam se qualificar para ocupá-lo, o espaço público era um espaço de

---

[235] ANTUNES , Marco António. **O público e o privado em Hannah Arendt.** Biblioteca on line de Ciências da Computação. Disponível em: http://www.bocc.ubi.pt/pag/antunes-marco-publico-privado.pdf

[236] ARENDT, Hannah. **Op. Cit.,** p. 58

liberdade perante os demais cidadãos, um espaço no qual o indivíduo podia agir de forma a demonstrar suas virtudes e afirmar sua individualidade entre seus pares, isto é, outros indivíduos que também houvessem alcançado essa condição econômica de superar a luta diária pela subsistência.

Não é possível, portanto, pensar a democracia grega a partir da noção atual de democracia como modelo de governo em que se garante a participação da maioria, respeitados os direitos das minorias. As discussões mais importantes da coletividade grega eram travadas unicamente pelos poucos admitidos a ingressar no espaço público, que era marcado pela possibilidade de uma ampla difusão das ideias e discursos dos cidadãos gregos, através da plena publicidade dos atos.

Era essencialmente a publicidade que, afastando os atos da esfera recolhida da privatividade, permitiria que os atos transcendessem aos próprios indivíduos que os criaram, garantindo sua permanência para a posteridade. Essa noção de necessidade de publicidade marca indelevelmente o espaço público, que dela necessita, porque sem ela não se alcança a posteridade.

A distinção entre o público e o privado no mundo antigo, assim, correspondia à oposição entre a relevância e a irrelevância, entre a permanência e a futilidade, entre a honra e a vergonha ou inutilidade.[237] Por isso, de um modo geral, o espaço público era o local das virtudes, onde se localizavam a liberdade e a igualdade entre os cidadãos, ao passo que o privado era o espaço mundano da satisfação das necessidades.

Entretanto, mesmo a despeito da manutenção da força da ideia de superioridade do público sobre o privado, tão cara aos gregos, nas diferentes configurações sociais que se sucederam, essa diferença foi sendo progressivamente diminuída, tendo perdido muito de sua importância após a queda do Império Romano, quando o público (ou pelo menos o aspecto político do espaço público) foi parcialmente substituído pelo sagrado, com a Igreja Católica assumindo o papel de oferecer a cidadania que anteriormente era outorgada pelo governo municipal[238].

Na idade média passa a haver uma alteração fundamental no âmbito do espaço privado, que deixa de ser relegado ao aspecto de irrelevância e passa a ser elevado à condição de local em que também ocorrem relações importantes e de interesse da coletividade, o que faz com que se passasse a enxergar também no espaço privado um local de exercício de virtudes.

---

[237] ARENDT, Hannah. **A condição humana. 10ª. Ed.** Rio de Janeiro: Forense Universitária, 2007. P. 83

[238] ARENDT, Hannah. Op. Cit. P. 43

De fato, uma das diferenças que se estabeleceu entre a figura da antiguidade clássica do *Pater familiae* e o senhor feudal é que este último poderia exercer justiça dentro de seu espaço privado, ao passo que essa noção era totalmente desconhecida para o chefe de família da antiguidade, que não conhecia leis ou justiça fora do espaço público. Assim, o espaço privado passou a ser também um local ocupado pelas virtudes antes reservadas unicamente ao espaço público, atraindo maior atenção e escrutínio para o que antes era excluído dos debates acerca da vida boa e do bem comum.

A modificação do *status* do espaço privado levou ao ajustamento de todas as atividades humanas, que passaram a seguir o molde familiar nas suas relações, gerando profundas consequências nas organizações profissionais, como as corporações de ofício e guildas, marcadas pela hierarquia[239], e até mesmo nas primeiras companhias comerciais, nas quais, como afirma Arendt, "o lar comum original parecia estar implícito na própria palavra (*companis*)"[240].

Para Rodotà[241], o fortalecimento do desejo de intimidade na Idade Média foi uma mudança radical que, ao alterar até mesmo a forma da casa, permitiu o afastamento, por vontade própria, da vida e das atividades comuns, marcando o início de um novo alinhamento de classes. A burguesia se diferenciou das demais classes pela possibilidade de aproveitar plenamente a própria intimidade, isolando-se não só dos demais estamentos sociais, mas inclusive de si própria, por isso que o surgimento das condições materiais para a intimidade guarda profundas ligações com a própria identidade de classe da burguesia no corpo social. O burguês, como afirma Rodotà, "apropria-se de um seu 'espaço', com uma técnica que lembra aquela estruturada para a identificação de um direito à propriedade 'solitária'"[242].

Houve assim uma profunda alteração na concepção do que se entendia como "privado", que gradativamente foi perdendo o sentido de privação da participação da comunidade política e passou a estar ligado à noção de proteção de uma esfera própria do indivíduo, separado da coletividade. A alteração do sentido de privacidade, que hoje remete a

---

[239] Vale notar que apesar de a organização da hierarquia interna das guildas e confrarias ter promovido a concentração de poder político e econômico em torno dos mestres, fomentando uma regulamentação de uma estrutura interna que favorecia as famílias mais tradicionais e reservando maiores ganhos e acesso aos mais próximos, essas instituições também sofreram forte influência dos poderes seculares e religiosos, numa relação de influência mútua. Sobre o tema, ver OLIVEIRA, Elizandro e REIS, Jaime. **O poder nas corporações de ofícios.** Anais do VIII Congresso Internacional de História. 2017. Disponível em http://www.cih.uem.br/anais/2017/trabalhos/3493.pdf

[240] ARENDT, Hannah. **A condição humana.** 10ª. Ed**.** Rio de Janeiro: Forense Universitária, 2007 P. 44

[241] RODOTÀ, Stefano. **A vida na sociedade da vigilância. A sociedade hoje.** Rio de Janeiro: Renovr, 2008, p. 26

[242] Idem, Ibidem, p. 27

um círculo de intimidade, é um acontecimento concomitante à elevação da posição valorativa conferida à noção de "privado", que foi enriquecida a partir do individualismo moderno[243].

A noção do privado como um espaço subalterno e inferior ao público, ligado fundamentalmente à ideia de igualdade, perdeu força com a ascensão do cristianismo, cuja moral sempre insistiu na ideia de que cada um deve cuidar de seus próprios afazeres. Com a ascensão da burguesia, a igualdade entre aqueles poucos admitidos aos espaços públicos passou a ser insuficiente, e a busca pela liberdade no mundo produtivo do trabalho e da circulação de mercadorias passou a ser a ideia reitora, fazendo com que, do mundo obscuro da privatividade, se verificasse o surgimento do social que, como lembra Arendt, não foi construído em oposição ao público, mas em contraste com o espaço privado doméstico[244] .

Com o avanço do capitalismo para seu estágio mercantilista, no qual os estados se estruturaram com um corpo militar e administrativo permanentes, os burgueses passaram a sentir a necessidade de fazer com que sua emancipação econômica também representasse uma emancipação política. Isso levou à necessidade de criação de um espaço social próprio para debate de temas como o intercâmbio de mercadorias e a regulação do trabalho (aspectos que, por estarem ligados à satisfação das necessidades, e não à vida boa aristotélica, anteriormente não pertenciam ao espaço público, mas unicamente à esfera privada).

Para Habermas[245], o ponto de partida histórico para a moderna concepção de privacidade como intimidade livre e plena é o fato de que a autocompreensão da razão pública passou a ser guiada pelas experiências procedentes da esfera íntima das pequenas famílias (unidade social que se contrapõe às grandes famílias da antiguidade). Foram exatamente as experiências privadas procedentes da subjetividade e o uso da razão pública como elemento de crítica que fizeram com que a privacidade assumisse seu sentido moderno.

O antigo sentido do privado, marcado pelas ideias de privação da esfera pública e de local "subalterno", voltado unicamente à necessidade de buscar a sobrevivência, cedeu espaço a uma nova concepção, onde as relações familiares passam a se refletir na polarização entre o Estado e o social[246].

---

[243] Idem, Ibidem. P. 48

[244] Para Arendt, "a privatividade moderna é pelo menos tão nitidamente oposta à esfera social – desconhecida dos antigos, que consideravam seu conteúdo como assunto privado – como o é a esfera política propriamente dita. O fato histórico decisivo é que a privatividade moderna, em sua função mais relevante – proteger aquilo que é íntimo – foi descoberta não como o oposto da esfera política, mas da esfera social, com a qual, portanto, tem laços ainda mais estreitos e mais autênticos". Op. Cit. P. 48

[245] HABERMAS, Jurgen. **Mudança estrutural da esfera pública**. p. 66

[246] GUIMARÃES, Juliana Depiné Alves .**Opinião pública e internet: uma discussão acerca do conceito de esfera pública habermasiana nos ambientes digitais.**

Neste espaço social, no qual a burguesia pretendia intermediar interesses com o Estado e resguardar sua autonomia, o *status* do homem na esfera privada passou a combinar os papéis de possuidor de mercadorias com o do *pater familiae*, o de proprietário com o de homem. Por isso, na modernidade, a esfera privada se desdobrou em planos mais elevados do que a mera intimidade reclusa e inferior que a caracterizou na antiguidade e passou a ser um dos componentes da autocompreensão da publicidade burguesa. Surgiu, assim, a esfera do social, marcado pela divisão entre as instâncias do Estado e da sociedade na discussão de temas de interesse da coletividade, ou seja, passou a haver uma divisão entre os temas coletivos discutidos pelo poder público e temas também de interesse coletivo discutidos no âmbito da esfera privada (que passou a contar ela própria com uma esfera de discussões de assuntos públicos relevantes).

Assim, a partir da Idade Média, com a crescente participação da burguesia nas discussões públicas, a antiga visão do privado como algo subalterno e inferior passou a dar lugar a uma até então inédita valorização dos espaços e negócios privados (aí incluído o campo do social) e acabou modificando a própria noção de esfera pública.

Habermas[247] define como "públicos" os acontecimentos que são acessíveis a qualquer pessoa, e a "esfera pública" como sendo aquela em que pessoas privadas se juntam enquanto um público. A esfera pública habermasiana, portanto, é um espaço que se desenvolve no campo das tensões entre Estado e sociedade, de modo que é justamente a partir do avanço da economia e suas formas de relações de mercado que surgiu a esfera do "social", na qual aparecem novas formas de autoridade, constituídas fora do âmbito da autoridade pública. Há uma certa transferência de competências públicas para entidades privadas e uma substituição do poder público por um poder social. Para Habermas, há uma crescente despolitização da esfera pública e a subversão da publicidade crítica (*Öffentlichkeit*) para uma publicidade manipulativa (*Publizaität*) [248].

Um dos traços mais marcantes de tal concepção de esfera pública é que ela se localiza no domínio privado, já que é constituída por pessoas privadas[249]. A esfera pública burguesa, assim, é formada por indivíduos privados que, em conjunto, debatem publicamente assuntos

[247] HABERMAS, Jürgen. **Mudança estrutural da esfera pública**. p. 65

[248] LUBENOW, Jorge Adriano**. A esfera pública 50 anos depois**: esfera pública e meios de comunicação em Jürgen Habermas em homenagem aos 50 anos de Mudança estrutural da esfera pública. **Trans/Form/Ação**, Marília , v. 35, n. 3, p. 189-220, Dec. 2012 . Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-31732012000300010&lng=en&nrm=iso

[249] HABERMAS, Jürgen. **Historia y crítica de La opinion publica. La transformación estrutural de La vida pública.** 5ª. Edición**.** Barcelona: Ediciones G. Gilli, 1997.

de interesse geral, funcionando como uma instância de controle e de legitimação do poder político exercido pelo estado administrativo.

A chegada da modernidade coincidiu historicamente com a transformação da preocupação individual com a propriedade privada em preocupação pública. O advento do "social" como espaço dentro da esfera privada no qual se debatem assuntos públicos, referentes ao interesse da coletividade (essencialmente relacionados ao trabalho e ao comércio de mercadorias) foi um processo concomitante ao declínio da família e ao surgimento da sociedade de massas, indicando

> [...] que os vários grupos sociais foram absorvidos por uma sociedade única, tal como as unidades familiares haviam sido agregadas por grupos sociais; com o surgimento da sociedade de massas a esfera do social atingiu finalmente, após séculos de desenvolvimento, o ponto em que abrange e controla, igualmente e com igual força, todos os membros de determinada comunidade.[250]

Para Habermas, a partir da Idade Média o espaço público foi sendo alterado e evoluiu passando por três fases distintas. A primeira, de caráter feudal ou representativo, era caracterizada pela neutralidade em relação aos critérios de público e privado. A segunda fase surgiu com a Modernidade e se baseou na distinção entre público e privado. Por fim, a partir de meados do século XIX, há uma terceira fase, na qual se verifica a interpenetração entre o público e o privado, entre Estado e sociedade, que acabou levando a uma espécie de "refeudalização da esfera pública"[251].

Vale notar que há um contraste entre a esfera política inicialmente estabelecida na Idade Média, decorrente do descolamento do social do espaço privado, e que se estendeu até meados do século XIX, e a esfera pública desta terceira fase, resultante do momento histórico que precedeu a implementação do modelo de democracia representativa, no qual a tentativa de assegurar a possibilidade (ainda que formal) de participação das massas no poder político fez com que a esfera pública passasse a ser permeada pelas discussões de poder, acirrando a tensão entre um poder público que garante as liberdade e uma sociedade econômica

---

[250] ARENDT, Hannah. Op. Cit. p. 50

[251] SILVA, Filipe Carreira da. **Habermas e a esfera pública: reconstruindo a história de uma ideia**. Sociologia, Problemas e Práticas, Oeiras , n. 35, p. 117-138, abr. 2001 . Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0873-65292001000100006&lng=pt&nrm=iso>. acessos em 04 maio 2020.

organizada de modo privado. Habermas, rememorando Böckenforde, ilustra essa tensão afirmando que[252]

> Com a formação do confronto entre "Estado" e "sociedade", coloca-se o problema da *participação* da sociedade no poder de decisão do Estado e em seu exercício [...] O Estado põe os indivíduos e a sociedade em liberdade civil, e nela os mantêm criando e assegurando uma nova ordem jurídica universal, porém os indivíduos e a sociedade não têm nenhuma liberdade *política*, isto é, não participam do poder de decisão política concentrado no Estado e não existe nenhuma possibilidade institucionalizada de influenciá-lo ativamente. O Estado como organização de dominação manteve-se como que em si mesmo, isto é, sociologicamente apoiado pela realeza, e, como tal, estava "separado", do ponto de vista organizacional e institucional, da sociedade representada pela burguesia

O desenvolvimento dessa esfera pública burguesa tem relação com dois fenômenos interligados: a existência das condições materiais necessárias ao desenvolvimento da intimidade e a busca de emancipação política pela burguesia, que desde cedo buscou fazer com que esse espaço de discussões públicas, composto por pessoas privadas (essencialmente pelos burgueses), fosse regulado como se estivesse acima das próprias autoridades públicas, de forma que as discussões sobre o mundo econômico, sobre as regras gerais acerca do comércio de mercadorias e do trabalho, se mantiveram como discussões basicamente privadas, mas publicamente relevantes[253].

Em grande medida essa transformação decorreu do fato de que as relações de trabalho e de comércio não mais puderam permanecer circunscritas à intimidade, aqui entendida como uma área reclusa da esfera privada. Isso levou à aceleração dessa mudança de concepção de esfera pública, na qual o *status* do homem privado combina o papel de possuidor de mercadorias com o de pai de família, levando ao desdobramento da esfera privada em planos mais elevados do que aqueles limitados à mera esfera da intimidade e formando a esfera social.

Esse novo espaço, a esfera social, tem como principal característica uma irresistível tendência e necessidade de crescer, sobrepondo-se e ocupando espaços que anteriormente eram assinalados às esferas do público e do privado. Para Arendt[254], a elevação da economia doméstica e das atividades caseiras à condição de tema público relevante, próprio da esfera

---

[252] HABERMAS, Jürgen. **Mudança estrutural da esfera pública**. São Paulo: Editora Unesp, 2014. P. 50

[253] HABERMAS, Jürgen. **Historia y crítica de La opinion publica. La transformación estrutural de La vida pública.** 5ª. Edición**.** Barcelona: Ediciones G. Gilli, 1997. P 65/66

[254] ARENDT, Hannah. **A condição humana** ..., p. 55

social, observável ao longo de três séculos, canalizou os processos da vida para a esfera pública. A esfera privada da família, plano no qual as necessidades da vida, da sobrevivência individual e da continuidade da espécie eram atendidas e garantidas, foi desconfigurada no momento em que o labor e as atividades econômicas de circulação de mercadorias se tornaram publicamente relevantes. Para Arendt,

> No instante em que o labor foi liberado das restrições que lhe eram impostas pelo banimento à esfera privada - e essa emancipação do labor não foi consequência da emancipação da classe operária, mas a precedeu - , foi como se o elemento de crescimento inerente a toda vida orgânica houvesse completamente superado e se sobreposto aos processos de perecimento através dos quais a vida orgânica é controlada e equilibrada na esfera da doméstica da natureza. A esfera social, na qual o processo da vida estabeleceu o seu próprio domínio público, desencadeou um crescimento artificial, por assim dizer, do natural; e é contra esse crescimento - que o privado e o íntimo, de um lado, e de outro o político (no sentido mais restrito da palavra) mostram-se incapazes de oferecer resistência.

A interpenetração entre público e privado, aliada à irrupção das massas, alteraram a esfera pública, que passou a compreender uma promessa de possibilidade de acesso de classes excluídas. O Estado passou a exercer atividades administrativas até então reservadas à iniciativa privada e aumentaram os custos públicos do consumo privado[255].

A polarização gerada entre esfera íntima e esfera social fez com que atividades que antes eram designadas para a formação social e provinham de instituições públicas passassem a ser desempenhadas por organizações privadas. Ao mesmo tempo, houve também uma mudança estrutural na família, que perdeu suas funções tradicionais, como a tarefa de prover garantias sociais passando a ser assumida precipuamente pelo Estado. Assim, as políticas públicas acabam por, de certa forma, "desprivatizar" a família.

Por outro lado, o descolamento de determinadas relações da esfera privada leva à elevação da esfera social, que apesar de surgir a partir da esfera privada, com ela não se confunde, estabelecendo-se como que um *tertium genus*. A ascensão do social leva à publicização do privado e a privatização do público, fazendo com que surja o problema de identificar o que é público e o que é privado, posto que as esferas passam a se

[255] OLIVEIRA, Vânia Aparecida Rezende de. **Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa**. Cad. EBAPE.BR, Rio de Janeiro , v. 8, n. 4, p. 782-788, 2010. Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1679-39512010000400013&lng=en&nrm=iso

interpenetrarem, provocando a falsa impressão de que tudo se torna público e tudo se torna privado.

A separação entre público e privado é trabalhada por Habermas em dois níveis[256], o dos sistemas e o do mundo da vida. No nível dos sistemas, a separação público/privado se dá entre o Estado (sistema público) e a economia capitalista (sistema privado). Já no nível do mundo da vida, a distinção se estabelece entre o espaço da participação política e da formação da opinião, que constitui a esfera pública, e a esfera privada. Vale notar, entretanto, que a institucionalização de papéis específicos faz com que haja uma vinculação entre tais esferas, de modo que o sistema público se vincula à esfera pública por meio dos papéis do cidadão e depois do cliente, relações essas realizadas principalmente no ambiente do poder, ao passo que o sistema privado e a esfera privada ligam-se pelos papéis do trabalhador e do consumidor, trocas essas realizadas no âmbito do dinheiro.

Entretanto, se, por um lado, público e privado permanecem como realidades sociais distintas, é inegável que tais esferas mantêm pontos de contato bastante próximos, relacionando-se e influenciando-se mutuamente. Como afirma Losekann[257], a esfera pública retira da esfera privada demandas que serão objeto do debate público. Por outro lado, os debates ocorridos no âmbito da esfera pública são incorporados à esfera privada, influenciando a vida cotidiana. Releva notar, ainda, que tampouco é possível se pensar em uma separação entre as esferas pública e privada a partir do conteúdo das temáticas, já que na realidade são as condições de comunicação modificadas que as diferenciam. Assim, o que define se um tema é público ou privado é a capacidade dos atores de articularem tal temática em um debate que seja relevante para o interesse comum, não havendo temas que sejam inerentemente públicos ou privados. Para Habermas[258],

> O limiar entre esfera privada e esfera pública não é definido através de temas ou relações fixas, porém através de *condições de comunicação modificadas.* Estas modificam certamente o acesso, assegurando, de um lado, a intimidade e, de outro, a publicidade, porém elas não isolam simplesmente a esfera privada da esfera pública, pois canalizam o fluxo de temas de uma esfera para a outra.

---

[256] GONZAGA, Ana Carolina Magalhães e COUTO, Dilnéia Rochana Tavares do. **A dicotomia do público/privado em Hannah Arendt e Jürgen Habermas: interações e reflexões à luz da teoria crítca contemporânea.** Complexitas - Rev. Fil. Tem., Belém, v. 2, n.2 , p. 18-33, jul./dec. 2017

[257] LOSEKANN, Cristiana **A esfera pública habermasiana. Seus principais críticos e as possibilidades do uso deste conceito no contexto brasileiro.** Pensamento Plural. 04, 37 - 57, janeiro/junho 2009 Disponível em: http://pensamentoplural.ufpel.edu.br/edicoes/04/02.pdf p. 43.

[258] HABERMAS, Jürgen. (HABERMAS, 1997, p. 98)

Neste ponto, é interessante notar que as análises de Habermas e Arendt parecem fundar-se numa visão de que os valores "liberdade individual" e "igualdade social" seriam auto-excludentes. Enquanto Hannah Arendt baseou suas análises na liberdade e singularidade de cada indivíduo, concebendo a esfera pública aristotélica como um local em que os homens deveriam mostrar suas melhores qualidades, Habermas investigou o surgimento do espaço público burguês sob a ótica da igualdade, tendo como principal referência a Idade Moderna e seus desdobramentos liberal e, posteriormente, social-democrata[259].

A ênfase da análise habermasiana ao valor igualdade fica bem evidente quando se nota que, mesmo a despeito de ter modificado alguns de seus conceitos ao longo do tempo, no prefácio à obra "Mudança estrutural da esfera pública", escrito em 1990, Habermas reforça que a igualdade de cidadania, alcançada de um modo geral no século XX, não afetou o caráter patriarcal da sociedade como um todo. Para ele, a alteração da relação entre esfera pública e esfera privada ainda deve ser compreendida a partir dos conceitos da crítica marxista da ideologia e da dominação, na medida em que a igualdade de direitos e de participação ampla na esfera pública ainda excluía mulheres e a "plebe", isto é, os homens dependentes[260].

As diferenças de foco entre as análises de Habermas e Arendt ensejam diversos questionamentos e abrem a possibilidade de uma rica discussão entre a oposição liberdade/igualdade, a qual inclusive tem relação direta com a compreensão dos direitos fundamentais. Entretanto, empreender tal discussão nos distanciaria muito dos objetivos a que nos propomos no presente trabalho. De fato, para a compreensão da evolução das ideias de público e privado e sua articulação com os valores de privacidade e liberdade, é suficiente neste momento perceber o movimento que levou a privatividade a deixar as esferas recônditas do espaço íntimo do lar, que era tido como insignificante do ponto de vista do interesse da coletividade, e a elevação da esfera privada à condição de palco de discussões relevantes.

A passagem do sombrio mundo do lar para a luz daquilo que é público alterou profundamente o significado de "público" e "privado", de modo que, se Arendt reforça a ideia de que o sentido moderno de privacidade como esfera da intimidade decorreu da alteração da própria concepção daquilo que é a privatividade, com Habermas, pode-se afirmar que a noção moderna de privatividade corresponde ao reconhecimento político e jurídico de que a sociedade conquistou o espaço público.

---

[259] BARBOSA-FOHRMANN. Ana P. **Algumas incursões sobre o significado de espaço público nos pensamentos de Hannah Arendt, Jürgen Habermas, Charles Taylor e Nelson Saldanha**. Diálogos Latinoamericanos n° 10. V. 1, 2005. PP. 73-97. Disponível em https://www.academia.edu/3323628

[260] HABERMAS. Jürgen. **Mudança estrutural da esfera pública. Prefácio à nova edição (1990).** p. 45.

A importância dos papéis desempenhados nas relações privadas, na sua interação dialética com os papéis exercidos pelos atores no espaço público, fez com que atualmente seja inegável a posição de destaque, no mínimo equivalente, conferida às esferas pública e privada. Arendt afirma que, do ponto de vista da privatividade, a distinção entre as esferas pública e privada está ligada à distinção entre o que deve ser exibido e o que deve ser mantido oculto, por isso o privado era aquilo que deveria ser ocultado. Havia, assim, uma assimilação entre o que era privado (e, portanto, ocultado) e o que era irrelevante. Essa assimilação entre privado e irrelevante perdurou por muitos séculos, sendo certo que "somente a era moderna, em sua rebelião contra a sociedade, descobriu quão rica e variegada pode ser a esfera do oculto nas condições da intimidade"[261]. A ascensão da privatividade, que passou a ser tida como local de relevo e merecedor de atenção por parte da coletividade, foi bem descrita por Baudrillard[262]:

> Isso pode ser visualizado na inversão de valor entre história e cotidianidade, entre esfera pública e esfera privada. Até os anos 60, a história se impõe como tempo forte: o privado e o cotidiano não são mais do que o avesso obscuro da esfera política. No melhor dos casos, intervém uma dialética entre os dois e pode-se pensar que um dia o cotidiano, como o individual, resplandecerá além da história, no universal. Mas até lá só se pode deplorar o recuo das massas a sua esfera doméstica, sua recusa da história, da política e do universal, e sua absorção na cotidianidade embrutecida do consumo (felizmente elas trabalham, o que lhes garante um estatuto histórico "objetivo" até o momento da tomada de consciência). Hoje, inversão do tempo fraco e do tempo forte: começa-se a vislumbrar que o cotidiano, que os homens em sua banalidade até que poderiam não ser o reverso insignificante da história - melhor: que o recuo para o privado até poderia ser um desafio direto ao político, uma forma de resistência ativa à manipulação política. Os papéis se invertem: é a banalidade da vida, a vida corrente, tudo o que se estigmatizara como pequeno-burguês, abjeto e apolítico (inclusive o sexo) que se torna o tempo forte; e é a história e o político que desenvolvem sua acontecimentalidade abstrata algures

O espaço privado, um espaço no qual o indivíduo pode desenvolver suas potencialidades livre da vigilância e controle da coletividade, um domínio de auto-desenvolvimento e de escolhas morais, no qual se desenvolve a vida cotidiana, ganha ares de elemento essencial para a vida em sociedade. A garantia de um espaço de proteção para a privacidade está ligada à possibilidade de livremente exercer direitos fundamentais. A

[261] ARENDT, Hannah. **A condição humana.** p. 82

[262] BAUDRILLARD, Jean. **À sombra das maiorias silenciosas O fim do social e o surgimento das massas.** São Paulo: Editora Brasiliense, 1985. p. 22

privacidade, portanto, tem um caráter instrumental, atuando como meio de proteção de outros direitos e valores. Liberdade, igualdade e até mesmo a democracia dependem da proteção à privacidade para que efetivamente possam florescer.

A visão da privacidade por uma perspectiva instrumental, ligada à proteção de outros direitos e valores, especialmente no campo da participação política, tem sido sustentada por Evgeny Morozov[263], para quem a questão relativa à privacidade é sobretudo política, e depende de uma solução cívica, a ser construída coletivamente a partir de uma ampla participação social que possibilite enxergar na proteção da privacidade um caminho para a proteção da liberdade, da igualdade e da própria democracia, já que as soluções centradas unicamente na perspectiva individualista da privacidade, como as de criação de mecanismos de pagamento pelo uso de dados privados ou a aprovação de leis acerca de privacidade, são insuficientes. Para ele, a privacidade não é um fim em si mesma, mas constitui um meio para se atingir um certo ideal de política e participação democrática, no qual os cidadãos sejam mais do que meros fornecedores de dados para tecnocratas e capitalistas sedentos por vigilância e controle.

A privacidade é parte importante de uma democracia, porque é ela que garante aos indivíduos a possibilidade de desenvolver e expressar sua própria opinião, livre da vigilância, controle e manipulação. Nessa perspectiva, a privacidade passa a ser vista também como um dos componentes fundamentais para a construção de um regime efetivamente democrático. Sem que se garanta a privacidade, não só a possibilidade de os indivíduos se manifestarem livremente no espaço público, mas também a possibilidade de construírem e desenvolverem suas convicções sem manipulações e influências, não se poderá efetivamente falar em democracia.

De fato, entre os fundamentos da democracia está o de que as decisões políticas devem ser tomadas levando em consideração os interesses de todas as pessoas, sendo certo que ninguém melhor do que o próprio indivíduo para julgar quais são seus próprios interesses e para defendê-los. A junção dessas duas ideias leva ao que Dahl[264] denomina de princípio forte da igualdade, que parte da crença de que nenhum dos membros de uma coletividade, isoladamente considerado, e tampouco alguma minoria, podem ser considerados como tão superiores a ponto de receber a autorização de toda a coletividade para governá-la. A democracia, ao levar em consideração o interesse de todas as pessoas, maximiza a liberdade

[263] MOROZOV, Evgeny. **The Real Privacy Problem.** MIT Technology review. Outubro de 2013. disponível em **https://www.technologyreview.com/2013/10/22/112778/the-real-privacy-problem/**

[264] CF. DAHL, Robert. **Democracia e seus críticos.** São Paulo : Editora WMF Martins Fontes, 2012**.** p. 47

garantindo direitos políticos básicos e direitos fundamentais como a liberdade de expressão e associação, permitindo que as pessoas, em suma, vivam sob as leis que elas próprias escolheram.

A democracia, portanto, pressupõe a possibilidade de escolha e, em uma sociedade na qual o indivíduo seja monitorado e vigiado constantemente, essa possibilidade é muito reduzida, tornando-se, na prática, quase inexistente, como já salientado no Capítulo 2, essa é cada vez mais a realidade vivenciada pela população na sociedade da informação. Um exemplo dado por Morozov[265] ajuda a compreender de que forma a diminuição da privacidade no mundo digital solapa a possibilidade de escolha.

Analisando as possibilidades do cruzamento de dados entre a geolocalização e o serviço de pesquisas semânticas Graph Search[266], que funcionou no Facebook até 2019, ele imagina a hipótese de um usuário ter pesquisado sobre restaurantes vegetarianos próximos ao local onde ele se encontra, o que poderia indicar a possibilidade de que o sujeito estivesse pensando em deixar de consumir carnes. O Facebook faz, então, em tempo real, um leilão entre indústrias de carne e indústrias de produtos veganos, para saber quem tem mais interesse nos dados daquele usuário. Uma vez que a indústria de carnes tenha obtido maior sucesso na aquisição dos dados do usuário, este passa a receber inúmeros "incentivos" para não alterar seus hábitos de consumo, como, por exemplo, a informação de que a seção de carnes no supermercado está com promoções, ou que a churrascaria local está oferecendo um desconto no jantar etc, até que, após algum tempo, o usuário acabe por decidir manter seus hábitos carnívoros. Assim, o que parece à primeira vista uma escolha livremente feita pelo indivíduo, acaba por se revelar em grande medida produto de uma série de "empurrões" e "incentivos" decorrentes da obtenção de dados pessoais que foram utilizados de acordo com uma estratégia comercial para regular comportamentos.

---

[265] MOROZOV. Evgeny. **Big tech. A ascensão dos dados e a morte da política.** São Paulo: Ubu Editora. 2018, pp. 32/32

[266] O Graph Search era um motor de pesquisa semântico, que apresentava resultados como respostas a pesquisas feitas em linguagem natural, a partir do cruzamento de dados mapeados dos usuários da plataforma (e que incluíam seus amigos e contatos na rede) com dados externos, obtidos do bing e de dados de geolocalização, para dar uma resposta específica para cada usuário. A ferramenta entrou em operação em março de 2013, teve sua visibilidade restrita em 2014 e foi praticamente desabilitada em junho de 2019, em meio a polêmicas sobre possíveis violações à privacidade dos usuários, ante a riqueza de dados que poderiam ser obtidos por meio das pesquisas por esse motor. Sobre o assunto, ver COX, Joseph. **Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies.** Motherboard, 2019. disponível em https://www.vice.com/en_us/article/zmpgmx/facebook-stops-graph-search

No mesmo sentido, em meados da década de 1980, um dos pioneiros campo da proteção de dados, Spiros Simitis[267] realçou a ligação entre privacidade e democracia, chamando atenção para o fato de que a participação democrática pressupõe interação constante entre as esferas pública e privada, sendo que a coleta e processamento de dados em massa possibilita uma verdadeira colonização da vida do indivíduo, colocando em risco a possibilidade da democracia.

Isso ocorreria por três razões: a primeira é o fato de que as questões relativas à privacidade não mais podem ser consideradas como problemas meramente individuais, mas antes expressam conflitos que afetam a todas as pessoas. Em segundo lugar, as novas tecnologias possibilitam gravar e reconstruir as atividades do indivíduo em detalhes, quase minuto a minuto do dia. Finalmente, essas informações são constantemente utilizadas para impor padrões de comportamento. Por isso, quanto maiores a automatização e a publicização da vida, mais evidente será a constatação de que a privacidade é um pré-requisito para a capacidade de participação do indivíduo no debate público. "Onde a privacidade é desmantelada, tanto as chances de avaliação dos processos políticos e sociais quanto a oportunidade de desenvolver e manter um particular estilo de vida se esvaem"[268].

A percepção do caráter instrumental da privacidade mostra o quanto ela é importante como meio de proteção aos direitos fundamentais. A própria evolução da noção de público e privado, da diferenciação necessária entre um espaço da coletividade e um espaço reservado para o indivíduo, demonstra a inter-relação entre privacidade e direitos fundamentais.

Nesse sentido, a ligação entre a proteção da privacidade e dos direitos fundamentais básicos como liberdade e igualdade não poderia ser mais íntima, sendo certo que alguns dos mais importantes direitos fundamentais, como os direitos da personalidade, as liberdades de crença e de consciência e expressão, o sigilo da correspondência, das comunicações e dos dados, a inviolabilidade da residência, bem como a proteção da família, caracterizam uma zona inviolável da integridade pessoal e da formação do juízo e da consciência. A própria existência da moderna sociedade civil, que é vinculada aos núcleos privados do mundo da vida, se apoia na necessidade de estruturas legais que possam demarcar pluralidade,

[267] SIMITIS, Spiros. **Reviewing privacy in an information society.** University of Pennsylvania Law Review. Vol. 135, n. 3. 1987. p. 734. Dispomnível em www.jstor.org/stable/3312079.

[268] Tradução nossa. No original: "Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade"

privacidade e publicidade, protegendo-as dos poderes políticos e econômicos. Não é por outra razão que Habermas[269] ressalta que

> O nexo estreito entre cidadania autônoma e esfera privada intacta revela-se claramente, quando a comparamos com sociedades totalitárias onde existe o socialismo de estado. Nelas, um Estado pan-óptico controla diretamente a base privada dessa esfera pública. Intervenções administrativas e supervisão constante desintegram a estrutura comunicativa do dia-a-dia na família, na escola, na comuna e na vizinhança. A destruição de condições vitais solidárias e a quebra da iniciativa e da independência em domínios que se caracterizam pela super-regulação e pela insegurança jurídica, implicam o aniquilamento de grupos sociais, de associações e de redes, a dissolução de identidades sociais através da doutrinação, bem como o sufoco da comunicação pública espontânea. A racionalidade comunicativa é destruída, tanto nos contextos públicos de entendimento, como nos privados

A extensão da proteção legal que cada sociedade confere à privacidade, entretanto, é algo muito dependente das circunstâncias concretas da sua própria evolução sócio-histórica, pois reflete os compromissos políticos definidos para aquela sociedade específica, dentro de um contexto muito específico. Aliás, cabe aqui ressaltar um traço particular da proteção legal à privacidade nas democracias. É que, se por um lado a proteção à privacidade é essencial para que direitos fundamentais democráticos possam se desenvolver livremente, por outro lado uma exacerbada proteção à privacidade pode asfixiar a própria existência da democracia.

Com efeito, a democracia pressupõe a possibilidade de participação dos indivíduos nas discussões públicas, o que, por seu turno, pressupõe a garantia de um certo nível de transparência e visibilidade das relações, a fim de possibilitar o necessário engajamento dos cidadãos nas discussões públicas relevantes.

Neste aspecto, vale ressaltar que, para Dahl[270], a moderna democracia representativa (por ele denominada poliarquia) é uma ordem política que se distingue por necessariamente contar com sete instituições:

1**. Funcionários eleitos.** Os funcionários eleitos são constitucionalmente investidos do controle político das decisões governamentais;

2. **Eleições livres e justas**. Os funcionários eleitos são escolhidos em eleições frequentes, conduzidas de modo justo, nas quais a coerção é relativamente rara;

---

[269] HABERMAS, Jürgen. **Direito e democracia: entre facticidade e validade.** Vol. II. Rio de Janeiro: Tempo brasileiro, 1997. p. 102

[270] DAHL, Robert. **Democracia e seus críticos.** São Paulo : Editora WMF Martins Fontes, 2012. p. 350/351

3. **Sufrágio inclusivo.** Praticamente todos os adultos têm o direito de votar na eleição dos funcionários do governo;

4. **Direito de concorrer a cargos eletivos**. Praticamente todos os adultos têm o direito de concorrer a cargos eletivos no governo, embora os limites de idade possam ser mais altos para ocupar o cargo do que para o sufrágio;

5**. Liberdade de expressão**. Os cidadãos têm o direito de se expressar, sem o perigo de punições severas, quanto aos assuntos políticos de uma forma geral, o que inclui a liberdade de criticar os funcionários do governo, o governo em si, o regime, a ordem socioeconômica e a ideologia dominante;

6. **Informação alternativa.** Os cidadãos têm o direito de buscar soluções alternativas de informação. Ademais, existem fontes de informação alternativa protegidas por lei.

7. **Autonomia associativa.** Para alcançar seus vários direitos, inclusive aqueles relacionados acima, os cidadãos também têm o direito de formar associações ou organizações relativamente independentes, inclusive partidos políticos independentes e grupos de interesse.

É interessante notar que, das sete instituições necessárias para a democracia apontadas por Dahl, três guardam relação direta com a proteção à privacidade, com a existência de uma esfera de atuação do indivíduo onde ele possa fazer suas próprias escolhas morais. A democracia efetiva, assim, depende da existência de um ajuste fino na proteção legal da privacidade que, ao mesmo tempo em que permita ao indivíduo estabelecer as condições para a construção e defesa de valores, interesses próprios e suas escolhas morais, livre da vigilância e do controle por parte de grupos sociais políticos e econômicos, também possibilite a efetiva participação dos indivíduos na vida pública e social. Assim, para a existência da democracia, a proteção à privacidade deve ser sempre balanceada com a necessidade de garantia de transparência.

A necessidade de que esse balanceamento entre privacidade e transparência esteja bem ajustado torna-se ainda mais imperiosa em tempos de rápida mudança tecnológica, como os que vivemos, em que, mais do que os aspectos técnicos ou econômicos, a questão política relacionada à privacidade desponta fundamental, devendo ser estabelecidos os seus limites no âmbito de um amplo debate público. Não é por outra razão que há um intenso e contínuo debate na sociedade atual acerca do papel e do valor da privacidade, bem como da extensão da proteção que o sistema legal deve conferir a ela. Na verdade, a extensão de tal proteção é um elemento sempre aberto à negociação entre os diversos atores sociais nas

modernas democracias, já que, como afirma Simitis, "longe de ser tida como um elemento constitutivo de uma sociedade democrática, a privacidade aparece como uma contradição tolerada, cujas implicações devem ser constantemente reconsideradas".[271]

3.2 A DIMENSÃO COLETIVA DA PRIVACIDADE

A privacidade é um direito fundamental que guarda íntima relação com liberdade, igualdade e democracia, por isso que, ao contrário da ideia amplamente difundida que a compreende unicamente como o direito de ficar só (ou, adotando-se uma tradução mais adequada para a expressão de Warren e Brandeis, o direito de ser deixado em paz), não se pode pensar a privacidade sob essa ótica individualista. Na realidade, mais importante ainda é reconhecer sua dimensão coletiva, que se torna essencial para a dignidade da pessoa humana. Essa compreensão, inclusive, foi expressamente reconhecida pela Ministra Rosa Weber no RE 1010606/RJ, quando afirmou que

> [...] a proteção da privacidade também é uma característica estrutural indispensável das sociedades democráticas. E isso porque tanto o reconhecimento de uma esfera de privacidade imune à ingerência quanto a garantia de salvo-conduto à palavra proferida surgiram, na história do constitucionalismo moderno, como fatores de limitação do poder das autoridades constituídas sobre os cidadãos. Se aos cidadãos não for assegurada uma esfera de intimidade privada, livre de ingerência externa, um lugar onde o pensamento independente e novo possa ser gestado com segurança, de que servirá a liberdade de expressão? [272]

A compreensão da existência de uma dimensão eminentemente coletiva da privacidade permite superar a visão reducionista de privacidade que a torna inadequada para tratar da efetiva proteção da dignidade da pessoa humana na sociedade contemporânea. De fato, essa visão reducionista, que praticamente reduz a privacidade à intimidade e, com isso, a compreende como a possibilidade de controle do fluxo de informações relacionadas ao indivíduo, acaba por tornar necessária a criação de um direito autônomo à proteção de dados. Nesse sentido, afirma Bruno Bioni que

---

[271] SIMITIS, Spiros. **Reviewing privacy in an information society.** University of Pennsylvania Law Review. Vol. 135, n. 3. 1987. p. 732. Dispomnível em www.jstor.org/stable/3312079. No original: "Far from being considered a constitutive element of a democratic society, privacy appears as a tolerated contradiction, the implications of which must be continuously reconsidered"

[272] BRASIL. SUPREMO TRIBUNAL FEDERAL. Voto da Ministra Rosa Weber no RE 1010606/RJ, p. 179.

> Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle das informações pessoais do que seja algo íntimo ou privado do sujeito. A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão, por exemplo.[273]

Entretanto, não se pode reduzir a privacidade à esfera da intimidade do indivíduo, o que equivale compreender a privacidade unicamente sob uma dimensão individual. O reconhecimento de uma dimensão coletiva da privacidade permite compreender que os dados do indivíduo, independentemente de sua publicização, continuam pertencendo à sua esfera de proteção. A tutela da privacidade não pode se reduzir à possibilidade de que o indivíduo limite o acesso ou exerça controle sobre a qualidade da informação sobre si, até porque, em razão da grande capacidade de processamento dos modernos sistemas de *big data*, mesmo informações anonimizadas (isto é, desvinculadas de elementos que permitam a identificação imediata da pessoa a quem o dado se refere) e corretas podem colocar em risco o espaço de livre desenvolvimento pessoal do indivíduo.

De fato, mesmo dados aparentemente inócuos, como por exemplo o número de placas de automóveis pelos estacionamentos privados, o registro de conexão do IP com o provedor de internet ou registros de pagamentos por meios digitais, ainda que anonimizados, podem ser processados em meio a inúmeros outros dados coletados massivamente, correlacionados com eles, e, assim, possibilitar a identificação da pessoa ou grupo a quem eles se referem. Isso faz com que o conceito de dado pessoal constante do artigo 5ª, I, da Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) perca um pouco do efeito protetivo pretendido.

Com efeito, a definição de dados pessoais constante da LGPD como a "informação relacionada a pessoa natural identificada ou identificável" replica o conceito do Regulamento Geral sobre a Proteção de Dados da União Européia (RGPD) 2016/679, que define dado pessoal como a

[273] BIONI, Bruno Ricardo. **Proteção de dados pessoais. a função e os limites do consentimento**. 2a. edição. Rio de Janeiro: Forense, 2020. p. 58

> informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;[274]

A amplitude do conceito, que abrange meios indiretos de identificação, faz com que dados como, *v.g*., endereços, caixas postais, números de telefone e endereços de IP possam ser considerados dados pessoais, já que é possível, por meio de consulta a bancos de dados ligar tais dados ao seu titular, identificando-o. Por isso, numa perspectiva ampla do que seja dado pessoal, tal como faz a LGPD e o RGPD (diretriz que também é seguida nos Estados Unidos da América com o conceito de *Personal Identifiable Information* - PII), estamos praticamente produzindo e fornecendo dados pessoais durante quase todos os momentos de nossa vida social. Daí porque o fato de um dado ter se tornado público ou de ele ter sido transferido ao domínio de um ente público não significa que ele deixe de ser relevante para a tutela da privacidade.

Na realidade, a dimensão coletiva da privacidade indica a necessidade de que ela seja compreendida a partir de uma concepção mais ampla, que possa superar a tradicional visão individualista desse direito. De fato, as teorias mais difundidas da privacidade a compreendem ou como a possibilidade de limitar o acesso de terceiros às nossas informações pessoais (privacidade como *restrição de acesso*, que a aproxima da noção de intimidade) ou como a possibilidade de assegurar ao titular do dado o direito de controlar a informação sobre si (*privacidade como controle).*

As teorias que defendem a concepção da privacidade como restrição de acesso ao espaço do indivíduo guardam muita proximidade com a tese original de Brandeis e Warren que definiam a privacidade como o direito de "ser deixado em paz" e decorrem do reconhecimento de um desejo imanente ao ser humano pela ocultação de determinadas situações e pela necessidade de ter momentos em que o indivíduo possa se manter afastado dos demais. A privacidade seria violada, assim, pela exposição pública de assuntos íntimos, que tenham sido previamente ocultados pelo interessado. Nas palavras de Richard Posner[275],

---

[274] CF. UNIÃO EUROPEIA. RGPD. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1

[275] Citado por SOLOVE, Daniel. **Understanding privacy.** Cambridge: Harvard University Pres, 2008. Disponível em http://ssrn.com/abstract=1127888. p. 21

> [A] palavra "privacidade" parece abranger pelo menos dois interesses distintos. Um deles é o interesse em ser deixado em paz — o interesse que é invadido pela solicitação telefônica indesejada, o caminhão de som barulhento, a música nos elevadores, ser empurrado na rua, ou mesmo um cartaz de teatro obsceno ou uma obscenidade gritada... . O outro interesse de privacidade, ocultação de informações, é violado sempre que informações privadas são obtidas contra a vontade da pessoa a quem as informações pertencem[276].

Essa concepção da privacidade como restrição de acesso foi, no Brasil, defendida por Celso Bastos, que a entende como a "faculdade que tem cada indivíduo de obstar a intromissão de estranho em sua vida particular"[277]. Bem ilustrativa desta concepção, que equipara os conceitos de intimidade e de privacidade, é a visão de José Raul Gavião de Almeida[278], para quem esta última "se liga ao conceito da intimidade como oásis da vida humana, onde se acolhem sentimentos e pensamentos fechados no coração e escondidos na mente. É onde se abriga o 'direito de estar só'".

Por outro lado, as teorias fundadas na concepção da *privacidade como controle* sobre os dados pessoais partem da ideia de que os dados são bens de propriedade do seu titular que, por isso, deve ter a possibilidade de exercer controle sobre eles, como expressão do domínio. Nessa linha, a força tarefa para a estrutura informacional formada pelo ex-presidente dos Estados Unidos, Bill Clinton, conceituou privacidade como sendo "a reivindicação de um indivíduo de controlar os termos sob os quais as informações pessoais - informações identificáveis ao indivíduo - são adquiridas, divulgadas e usadas." [279]

São teorias de forte cunho privatista, que refletem a ideia de que o indivíduo deve ser o proprietário de seus dados. Apesar da imagem da privacidade como expressão da propriedade ter sido inicialmente tratada nos escritos filosóficos de John Locke[280], para quem os indivíduos têm direito à própria pessoa e aos frutos de seu trabalho, a tradução desse conceito a uma teoria jurídica da privacidade provavelmente remonta ao clássico e influente

---

[276] Tradução nossa. No original: [T]he word "privacy" seems to embrace at least two distinct interests. One is the interest in being left alone—the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theater billboard or shouted obscenity.. . . The other privacy interest, concealment of information, is invaded whenever private information is obtained against the wishes o f the person to whom the information pertains.

[277] BASTOS, Celso.**Curso de Direito Constitucional**. São Paulo: Saraiva, 2001. p. 203

[278] ALMEIDA. José Raul Gavião. **Anotações acerca do direito à privacidade**. *in* MIRANDA, Jorge e SILVA, Marco Antonio Marques (cord). **Tratado luso-brasileiro da dignidade humana.** 2a. edição. São Paulo: Quartier Latin, 2009. p.720

[279] SOLOVE, Daniel. **Understanding privacy.** p. 24. Tradução nossa. No original : "an individual's claim to control the terms under which personal information - information identifiable to the individual - is acquired, disclosed, and used."

[280] CF. SOLOVE, Daniel. **Op. Cit.** p. 26 e ss.

trabalho Privacy and Freedom, publicado em 1967 por Alan Westin[281], que definiu privacidade como "a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros"[282].

Tais teorias estão muito ligadas ao conceito de autonomia informacional ou *autodeterminação informativa*, utilizado pela primeira vez em uma decisão proferida em 1983 pelo Tribunal Constitucional Alemão. Naquele caso, a Corte discutia a constitucionalidade da Lei do Censo Alemã, que havia imposto aos cidadãos a obrigação de fornecer vários dados pessoais para possibilitar que a distribuição da população fosse mensurada estatisticamente. Ocorre que a lei também previa a possibilidade de que os dados obtidos fossem cruzados com outras informações constantes de bancos de dados públicos com uma genérica finalidade de "comparação de dados levantados com registros públicos e transmissão de dados tornados anônimos para repartições federais, estaduais e municipais para determinados fins de execução administrativas"[283]. Os termos amplos em que a lei fora redigida ensejou várias reclamações constitucionais, que levaram a Corte a declarar sua inconstitucionalidade parcial, determinando que os dados coletados somente poderiam ser utilizados para a finalidade específica de recenseamento.

A Corte Constitucional Alemã, naquele julgado, afirmou o direito do cidadão de ter o controle de seus dados pessoais, cunhando a expressão "autodeterminação informacional ou autodeterminação informativa", criando assim um novo direito autônomo, por muitos tido como apartado da privacidade. Partindo do pressuposto de que os avanços tecnológicos acarretam um progressivo aumento da qualidade das informações coletadas, impactando significativamente nas liberdades individuais, o tribunal extraiu do direito geral da personalidade o direito autônomo de autodeterminação informativa, entendendo que o direito do indivíduo de autodeterminar seus dados pessoais estaria compreendido no direito de o indivíduo desenvolver sua personalidade livremente.

A decisão apontou a necessidade de se superar a dicotomia sigilo-publicidade, que não seria mais suficiente para resolver questões associadas à circulação de informações pessoais, e considerou que todo tratamento de informações pessoais afeta o direito à autodeterminação informativa. Para Bruno Bioni, o fato de a Corte Constitucional Alemã ter construído a noção de autodeterminação informativa como um direito autônomo, apartando-se das construções

[281] WESTIN, Alan. **Privacy And Freedom**, new York: Ig Publishing, 1967. (Ebook), p. 24

[282] Tradução nossa. No original: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

[283] CF. BIONI, Bruno Ricardo. Op. Cit. p. 97 e ss.

baseadas na dicotomia público-privado, representa um avanço, pois afasta-se da necessidade de comprovação da existências de aspectos lesivos na utilização dos dados, tornando desnecessária, para a proteção de dados, a verificação de se tratar de dado sensível ou saber se eles estariam relacionados a algo íntimo e sigiloso da pessoa. Nesse sentido, Bioni[284] afirma que

> [...] a fundamentação construída pelo julgado sob análise - Lei do recenseamento de 1983 - é paradigmática ao não tomar a proteção de dados pessoais como uma evolução do direito à privacidade. Pelo contrário, tratá-lo como um direito de personalidade autônomo, que reclama uma técnica de proteção desconectada da dicotomia entre público e privado.
> [...] Tal aspecto se não é por vezes omitido, não angaria, ao menos, o merecido destaque por parcela da doutrina que estabelece a proteção de dados pessoais como uma evolução do direito à privacidade.

Evidentemente, a dicotomia público-privado, entendida como um reflexo da distinção entre publicidade-sigilo, para afastar a tutela de dados e informações que já haviam sido tornadas públicas pelos seus titulares, é absolutamente incapaz de apreender toda a enorme complexidade da proteção à privacidade e a superação desse paradigma é um claro avanço na tutela de aspectos fundamentais da dignidade humana.

Entretanto, isso apenas reforça o fato de que a privacidade é um objeto extremamente complexo e multifacetado. Assim, o argumento que sustenta a necessidade de compreensão da proteção de dados pessoais como direito autônomo e apartado da privacidade somente pode ser acolhido se a concepção da privacidade for aquela restrita à noção que a entende como reflexo do direito de propriedade dos dados e, portanto, a define como o direito do titular de controlar seus dados pessoais (privacidade como controle).

Neste ponto, cabe ressaltar que é completamente compreensível que Bioni aponte sua crítica para esta dada visão da privacidade, já que ela de fato é a mais usualmente utilizada pelos teóricos da privacidade. No Brasil, esta concepção também tem tido muita aceitação na jurisprudência, inclusive do Supremo Tribunal Federal. Nesse sentido, a autodeterminação informativa, como aspecto da privacidade relacionado ao controle do indivíduo sobre os próprios dados, foi expressamente reconhecida pelo STF no julgamento da medida cautelar na ADI 6387[285]

---

[284] BIONI, Bruno Ricardo. **Proteção de dados pessoais. a função e os limites do consentimento**. 2a. edição. Rio de Janeiro: Forense, 2020. p. 100.

[285] BRASIL. SUPREMO TRIBUNAL FEDERAL. ADI 6387 MC-Ref. Tribunal Pleno. Rel. Min. Rosa Weber. Julgado em 07.05.2020. Disponível em https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false

EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. **1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.** 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados

> específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada."

Mesmo a despeito da força que tal concepção tem angariado na doutrina e na jurisprudência, ela se mostra insuficiente para dar conta de toda a imensa complexidade da sociedade contemporânea, onde o capitalismo informacional assumiu a condição de modelo organizacional econômico por excelência e a obtenção, circulação, tratamento e comercialização de dados fazem parte do dia a dia da população.

De fato, é completamente irreal, na sociedade atual, se imaginar a possibilidade de que os titulares de dados efetivamente possuam algum controle sobre aquilo que cedem às empresas de tecnologia, posto que, no mundo real, no mais das vezes os usuários aceitam *cookies* e confirmam todas as configurações de privacidade solicitadas sem sequer imaginar o que de fato estão cedendo. Isso vale para sítios na internet, aplicativos de celular, aparelhos de televisão conectados à rede mundial e cadastros em farmácias, supermercados e postos de gasolina, por exemplo. Na enorme maioria das vezes o usuário sequer sabe o que efetivamente significa aquela concordância e, mesmo que soubesse, tampouco teria condições reais de negá-la, posto que isso quase sempre implica ou na negação do serviço ou no cancelamento de eventuais descontos no valor cobrado pelo serviço ou produto.

Um outro problema da concepção da privacidade como controle do indivíduo sobre seus dados pessoais reside no fato de que ela parte do pressuposto de que os dados são uma propriedade individual, uma *commodity* cuja titularidade cabe ao indivíduo. Como já afirmado quando da análise da metáfora dos dados como o novo petróleo (cap. 1.8), os dados são essencialmente diferentes de propriedades materiais. Em primeiro lugar, porque não são propriamente consumíveis, mas consistem em bens não rivais, dado que seu compartilhamento não leva à diminuição ou exclusão da informação originária. Ademais, essa visão olvida o caráter social que a informação possui. Os dados pessoais muitas vezes são criados a partir de relações sociais que somente existem a partir do contato com outras pessoas, o que gera dificuldades até mesmo quanto à correta identificação do titular do dado.

Solove[286] apresenta como exemplo as informações de navegação na internet, que são criadas a partir da conjugação das ações do usuário com os *websites*. Ele lembra que o valor da informação no ciberespaço muitas vezes é criado a partir da interação do indivíduo com terceiros, como ocorre na categorização e consolidação de dados pessoais para efeito de propaganda direcionada.

Por isso, essa visão da privacidade como controle por parte do indivíduo não é adequada para a compreensão da privacidade na sociedade contemporânea. Aliás, vale ressaltar que, como lembra o Ministro Dias Toffoli em seu voto no RE1010606/RJ[287], que tratou o direito ao esquecimento, a Corte Constitucional Alemã, no julgamento da Lei do recenseamento de 1983, já alertava que

> o direito à autodeterminação informacional que ali se afirmava não era absoluto (…) não [era] um direito isolado, mas ligado à comunidade, afastando uma noção individualista e afirmando que o indivíduo deveria aceitar certo limites à sua autodeterminação informacional por razões de interesse público.

Ademais, deve se salientar que de fato a dicotomia público/privado é insuficiente para dar conta de toda a complexidade das relações e da necessidade de proteção ao indivíduo enquanto membro da coletividade e da própria sociedade, que para florescer precisa contar com um conjunto de indivíduos aos quais seja garantido espaço individual para criar sua própria identidade, desenvolvendo e manifestando seus pensamentos. A própria história da evolução do público e do privado, tratada na seção 3.1 do presente capítulo, demonstra de forma muito clara o quanto variaram ao longo da História não só os limites do que é público e do que é privado, mas principalmente o valor que era conferido a cada uma dessas esferas e quais os valores subjacentes à esfera privada.

Por isso, é claramente insuficiente reduzir-se a privacidade a seu aspecto individual e privatístico. A rigor, a privacidade não é privada, no sentido de que não se pode pensar a privacidade como um tema unicamente relacionado ao direito privado, ou referente a relações eminentemente privadas. Nesse sentido, é absolutamente compreensivo que muitos autores, como Bioni, comemorem a superação da dicotomia público-privado no tratamento da proteção de dados e, acrescento, da privacidade. Na realidade, porém, uma compreensão da dimensão coletiva da privacidade é suficiente para afastar tanto a sua redução ao aspecto da

[286] SOLOVE, Daniel. **Understanding privacy.** Cambridge: Harvard University Pres, 2008. Disponível em http://ssrn.com/abstract=1127888.

[287] BRASIL. SUPREMO TRIBUNAL FEDERAL. RE 1010606/RJ. Voto do Ministro Dias Toffoli, p. 39. J. em 11/02/2021. Disponível em https://jurisprudencia.stf.jus.br/pages/search/sjur446557/false

intimidade, do sigilo, quanto sua redução ao aspecto de controle das informações pelo titular dos dados.

Essa compreensão não significa, por óbvio, que tais aspectos da privacidade sejam inexistentes ou que tais visões estejam incorretas. Na realidade, o que se afirma aqui é que as concepções da privacidade como direito de limitar o acesso ou da privacidade como direito de controlar a circulação de dados pessoais são apenas dimensões da privacidade que reverberam uma concepção individualista que, sem embargo de sua importância, não é suficiente para explicar todo o fenômeno. De fato, a possibilidade de criar um espaço de isolamento e limitação do acesso de terceiros a determinados aspectos da intimidade do indivíduo constitui evidente aspecto fundamental da privacidade. Da mesma forma, é inegável a importância de que o indivíduo possa controlar as suas informações que sejam acessadas por terceiros. Entretanto, por mais importantes que sejam tais aspectos, eles não esgotam a privacidade.

Por isso, é preciso lançar mão de uma abordagem menos restritiva de privacidade. Daniel Solove[288] sustenta a necessidade da reconstrução do conceito de privacidade a partir da teoria linguística de *semelhança de família* desenvolvida por Wittgenstein. Segundo o filósofo austríaco, em algumas situações a melhor compreensão da linguagem não se dá quando buscamos a essência de uma palavra ou expressão, para torná-la mais exata, posto que o significado decorre de uma ligação direta entre a palavra e a coisa a que ela se refere. Antes, o significado de uma palavra decorre da maneira com que ela é utilizada na linguagem cotidiana, por isso que algumas palavras e expressões não têm uma essência, mas várias, e assim certos conceitos retiram seu significado de um conjunto comum de características similares, formando uma "complicada rede de semelhanças sobrepostas e cruzadas: às vezes semelhanças gerais, às vezes semelhanças de detalhes"[289]. A privacidade seria um desses conceitos, já que ela tem várias dimensões que se entrelaçam e cruzam sem que necessariamente estejam unidas por um denominador comum.

Nesse sentido, uma abordagem extremamente interessante e capaz de articular a compreensão da privacidade tanto em suas dimensões individuais quanto na dimensão coletiva é a teoria da privacidade contextual de Helen Nissenbaum. Para ela, a privacidade nem pode ser entendida como o direito à intimidade e nem tampouco como o direito ao

[288] SOLOVE, Daniel. **Understanding privacy.** Cambridge: Harvard University Press, 2008. Disponível em http://ssrn.com/abstract=1127888.

[289] Idem, Ibidem. p. 42. Tradução nossa. No original: "complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail."

controle dos dados pessoais, mas antes deve ser entendida como o direito ao *fluxo apropriado* das informações pessoais[290].

A sociedade contemporânea vem experimentando profundas alterações no fluxo das informações, afetando instituições, estruturas de poder, relacionamentos etc. Nissenbaum, com a teoria da integridade contextual, procura criar meios de possibilitar que legisladores e reguladores tenham elementos para compreender e a lidar adequadamente com a ansiedade, o medo e os protestos que essas alterações radicais no fluxo de informações provocam. Ela busca fazer isso ressaltando a necessidade de que as expectativas das pessoas quanto ao tratamento de seus dados, de acordo com os padrões e as normas de comportamento socialmente aceitáveis, sejam levadas em conta, de forma a possibilitar que se determine, detecte ou reconheça quando uma violação às expectativas razoáveis ocorreu. Essa visão não rejeita as dimensões individualísticas de acesso e controle, mas antes visa a agregar um instrumental mais rico e aberto ao contexto fático para a correta compreensão e endereçamento dos problemas relacionados à privacidade.

Segundo Nissenbaum, a discussão sobre se a privacidade é direito de acesso ou direito de controle pode ser superada pela adoção da tese da integridade contextual. A ideia de que a privacidade consiste na possibilidade de limitação de acesso de outras pessoas a determinadas informações e dados pessoais se sobrepõe muitas vezes à ideia de norma de adequação informacional que está na base da tese da privacidade contextual, já que são exatamente essas normas sociais que delimitam as expectativas razoáveis sobre os dados compartilhados, e são elas que, ao fim e ao cabo, possibilitam ao indivíduo especificar sobre o que, sobre quem ou contra quem ele vai compartilhar informações.

Da mesma forma, o controle sobre os dados compartilhados ainda desempenha um importante papel na tese da privacidade contextual, já que configura um dos princípios da transmissão e do compartilhamento de dados. Por isso o controle é, sem dúvida, um aspecto de extrema importância na compreensão da privacidade, mas não pode assumir a condição de elemento único ou mesmo o papel de elemento central na definição do direito à privacidade.

Na verdade, ainda que muitas teorias e a jurisprudência sejam construídas em torno da noção da privacidade como controle pelo titular acerca dos próprios dados compartilhados com terceiros, ele é apenas um dos aspectos a ser levado em conta para avaliar a adequação da

[290] Nissenbaum. Helen. **Privacy in context. Technology, policy and the integrity of social life** Stanford: Stanford University Press, 2010.

transmissão do dado, de acordo com o contexto em que esse compartilhamento/tratamento ocorreu. Como afirma Nissenbaum[291], o controle

> [...] é apenas um entre muitos princípios de transmissão possíveis, que, por sua vez, são apenas um dos parâmetros que determinam se as normas informacionais foram respeitadas. Assim, saber se o controle é apropriado ou não, vai depender dos contextos, dos tipos de informação, do assunto, do remetente e do destinatário.[292]

Uma compreensão multidimensional da privacidade respeita os aspectos essenciais de sua dimensão individual, como a proteção a um espaço de solitude e intimidade protegido do acesso, do olhar ou da intromissão de outros, e a proteção à possibilidade de assegurar ao titular dos dados o controle das informações que ele compartilhou (conscientemente ou não). Porém, a abordagem multidimensional agrega a essas concepções também a noção de que essa avaliação da privacidade deve ser feita tendo em conta as normas sociais que determinam, em um dado contexto de tempo e local, quais são as expectativas razoáveis de tutela. Essa abordagem permite emprestar à privacidade uma compreensão mais adequada ao mundo contemporâneo, tornando-a um direito suficientemente forte a ponto de possibilitar a tutela da dignidade humana, da liberdade, da igualdade e da democracia, como também lhe confere flexibilidade suficiente para permitir compreender sua restrição em determinados contextos.

Isso é de extrema importância quando se pensa na privacidade em um contexto de sociedade da informação, em que a difusão do capitalismo de vigilância gera inúmeros novos desafios para o estado democrático de direito, especialmente quando se imagina a relação entre *surveillance* e direito penal.

---

[291] Nissenbaum. Helen. **Privacy in context. Technology, policy and the integrity of social life** Stanford: Stanford University Press, 2010. p. 148

[292] Tradução nossa. No original: " it is but one among many possible transmission principles, which in turn are but one of the parameters determining whether informational norms have been respected. Accordingly, whether or not control is appropriate depends on the contexts, the types of information, the subject, the sender, and recipient."

4. SURVEILLANCE E DIREITO PENAL

> *– Como imagina que vai ser o final? - perguntou o sacerdote.*
> *– Antes julgava que deveria terminar bem – disse K. – Agora, às vezes até eu mesmo duvido disso. Não sei como vai terminar. Você sabe?*
> *– Não – disse o sacerdote – mas temo que vá terminar mal. Consideram-no culpado. Talvez seu processo não ultrapasse nem mesmo um tribunal de nível inferior. No momento, pelo menos, consideram provada a sua culpa.*
> *– Mas eu não sou culpado – disse K. – É um equívoco. Como é que um ser humano pode ser culpado? Aqui somos todos seres humanos, tanto uns como os outros.*
> *– É verdade – disse o sacerdote. – Mas é assim que os culpados costumam falar.*
> *(Franz Kafka, O processo)*
>
> *Dê-me seis linhas escritas pelo mais honesto dos homens e eu acharei nelas um motivo para enviá-lo para a forca. (Cardeal Richelieu)*

A primeira vez que se teve notícia da utilização de computadores para orientar a atividade de policiamento ocorreu em Nova York, em agosto de 1965, na operação *Corral* (sigla para *Computer Oriented Retrieval of Auto Lacernists, "*identificação de ladrões de automóveis por meio de computador"). A operação pretendia monitorar as placas dos carros que atravessavam a ponte que liga a ilha de Manhattan ao Bronx, checando as informações em um computador Univac 490, máquina que à época custava cerca de US$ 500.000,00 e que tinha em seu banco de dados informações de 110 mil placas de carros roubados ou com pendências com a polícia[293].

Em uma época muito anterior ao surgimento da internet ou de qualquer rede de computadores, a alimentação do sistema era feita manualmente, com um policial em uma viatura estacionada na entrada da ponte transmitindo, via rádio, os números das placas dos carros para a estação onde ficava o operador do computador. O operador alimentava o computador com os dados da placa e em cerca de 7 segundos o sistema fazia a checagem do

[293] MOROZOV, Evgeny. **Big Tech. A ascensão dos dados e a morte da política.** São Paulo: Ubu Editora, 2018. p. 81 e ss.

banco de dados. Momentos após o início da operação, o sistema apresentou um resultado positivo (*match*) e uma equipe de 12 policiais que ficava na outra extremidade da ponte foi acionada para parar o automóvel e abordar seu condutor. Ao chegarem ao local, acompanhados de 125 jornalistas que cobriam o lançamento da operação, eles se depararam com uma dona de casa de 34 anos de idade que estava indo passar a manhã na praia. A razão pela qual o sistema apresentou resultado positivo foi que 15 meses antes ela havia passado em um sinal vermelho e tinha deixado de atender à intimação judicial.

Esse episódio soa até pitoresco quando visto com os olhos de hoje, diante da naturalidade com que encaramos a possibilidade de que nossos dados sejam quase instantaneamente acessados pelas modernas formas de coleta, inclusive câmeras e radares de velocidade que registram as placas de todos os veículos avistados. Entretanto, na essência, o episódio serve de alerta para os riscos inerentes à moderna *surveillance* e sobre como o aumento exponencial da capacidade de coleta, tratamento, transferência e utilização de dados dos indivíduos pode impactar os direitos fundamentais dos cidadãos diante do Estado em matéria penal.

Vivemos uma época em que praticamente todos os aspectos de nossas vidas passaram a ser mediados pela informática, e a vigilância se tornou uma constante. De fato, dia após dia está sendo formada uma extensa rede de dados à disposição dos agentes estatais encarregados da persecução penal e tal rede tende a aumentar exponencialmente com a proliferação dos sistemas de reconhecimento facial conjugados com o aumento da capacidade de coleta e processamento de dados coletados na internet. A vigilância por câmeras transformará pessoas desconhecidas em suspeitos conhecidos, não somente fornecendo o nome e os antecedentes criminais, mas também detalhes da história pessoal, postagens em redes sociais, contatos frequentes e dados sobre o histórico da sua localização, que poderão ser conjugados para serem utilizados como indícios da prática de crimes. Além disso, as correlações estabelecidas a partir das informações coletadas e processadas pelas ferramentas de inteligência artificial e *big data* poderão permitir a identificação de padrões de comportamento, possibilitando "classificar" o indivíduo como suspeito, a partir de seu comportamento anterior. Como lembra Andrew Ferguson[294], as forças encarregadas da persecução penal no mundo inteiro já utilizam softwares preditivos de policiamento para identificar áreas de maior probabilidade de ocorrência crimes e, assim, possibilitar uma melhor alocação do policiamento, mas, em breve,

[294] FERGUSON. Andrew Guthrie. **Big data and predictive reasonable suspicion.** University of Pennsylvania Law review. Vol. 163 nº 2. 2015, p. 351

as informações de *big data* darão um passo adiante e poderão permitir a "previsão" de ações criminosas ou até mesmo a probabilidade de que um dado indivíduo irá praticar um crime.

No limite, seria possível pensar não só no uso da tecnologia para possibilitar uma alocação mais eficiente de recursos humanos e materiais, que deveriam ser destacados para as áreas mais propensas a apresentar altos índices de criminalidade, mas até mesmo na reunião de elementos que poderiam chegar ao ponto de serem utilizados como fundamento para solicitação de autorização judicial para a realização de ações mais intrusivas, como buscas e apreensões, prisões cautelares ou mesmo condenações, aproximando-se de um cenário como o retratado no filme Minority Report, de 2002.

Por isso, pensar o futuro do direito penal e das liberdades constitucionais do indivíduo ante o Estado passa necessariamente pela definição dos limites do espaço legítimo de utilização das informações decorrentes da análise de dados estatisticamente relevantes coletados na rede mundial de computadores para efeito de persecução penal.

À primeira vista, pode até parecer que se está tratando de questões que (ainda) parecem distantes, como a predição de crimes, por exemplo. Entretanto, o policiamento preditivo é cada vez mais uma realidade. Em 2011, o Departamento de Polícia da Cidade de Los Angeles iniciou um programa de predição criminal denominado LASER (*Los Angeles Strategic Extraction and Restoration* - "Extração Estratégica e Restauração de Los Angeles"), que utilizava registros de inquéritos, prisões, interrogatórios e entrevistas e anotações feitas pelos policiais como fonte de informação, alimentando um algoritmo de inteligência artificial que supostamente deveria prever onde futuros crimes seriam cometidos e quem seriam os autores. O programa foi encerrado após cerca de 5 anos, quando ficou evidente não só a imprecisão de seus resultados, mas também que eles eram racialmente distorcidos, apresentando uma clara tendência para a "predição" de negros e hispânicos como criminosos e levando ao sobrepoliciamento das áreas por eles habitadas[295].

Com o progressivo avanço da inteligência artificial e a extensa coleta de dados, cada vez mais iniciativas como essas passam a ser apresentadas como a solução ideal para o grave problema da criminalidade, com seus entusiastas (principalmente de áreas técnicas) afirmando que bastaria resolver os problemas dos vieses na alimentação. Nesse sentido, recentemente os engenheiros da computação Shah e Bhagat[296] publicaram um estudo que tinha como objetivo

[295] THE GUARDIAN. **TechScape: can AI really predict crime?** 22 de dezembro de 2021. Disponível em https://www.theguardian.com/technology/2021/dec/22/techscape-lapd-operation-laser

[296] SHAH, N., BHAGAT, N. e SHAH, M. **Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention**. *Vis. Comput. Ind. Biomed. Art.* 09 de abril de 2021. disponível em https://doi.org/10.1186/s42492-021-00075-z

> [...] determinar como a combinação de ML [*machine learning*] e visão computacional pode ser utilizada pelas agências governamentais e autoridades para detectar, prevenir, e solucionar crimes a uma taxa muito mais precisa e rápida. Em suma, ML e visão computacional podem trazer uma evolução aos encarregados da persecução penal.

Levando esse tipo de abordagem ao limite, reeditando a criminologia lombrosiana com o uso da tecnologia, Jonathan Korn, Nathaniel Ashby, Roozbeh Sadeghian, professores da Universidade de Harrisburg, divulgaram em maio de 2020 os resultados de uma pesquisa intitulada "A Deep Neural Network Model to Predict Criminality Using Image Processing."[297] ("Um modelo de rede neural profunda para prever crimes usando processamento de imagem"), na qual sustentam terem desenvolvido um algoritmo de reconhecimento facial que, com 80% de acurácia e sem viés racial, seria capaz de prever se determinada pessoa iria cometer um crime. Segundo eles,

> Ao automatizar a identificação de ameaças potenciais sem viés, nosso objetivo é produzir ferramentas para prevenção do crime, aplicação da lei e aplicações militares que sejam menos impactadas por vieses implícitos e respostas emocionais,[298]

A publicação gerou uma enorme onda de reações negativas, culminando com uma carta pública, assinada por mais de 2400 pesquisadores da ciência da computação, sociólogos, historiadores, juristas, antropólogos e comunicólogos, condenando a pesquisa e afirmando, em suma, que as premissas científicas da pesquisa (utilização de dados biométricos para predição de comportamentos) já foram superados há muito tempo e que é impossível prever o comportamento criminoso sem viés racial porque a própria categoria "criminalidade" é racialmente enviesada. Os signatários da carta, que fundaram um grupo denominado *Coalition for Critical Technology*, afirmam que os dados gerados pelo sistema de justiça criminal não devem nunca ser utilizados para predição de comportamento criminal, já que as tecnologias de predição de crimes reproduzem injustiças e causam danos sociais reais. Na mesma linha do que afirmamos no capítulo anterior acerca da não neutralidade das tecnologias, eles salientam que[299]

---

[297] **HU facial recognition software predicts criminality.** Harriton University Press Release. Disponível em http://archive.is/N1HVe

[298] Tradução nossa. No original: "By automating the identification of potential threats without bias, our aim is to produce tools for crime prevention, law enforcement, and military applications that are less impacted by implicit biases and emotional responses"

[299] COALITION FOR CRITICAL TECHNOLOGY. **Abolish the #TechToPrisonPipeline.** Disponível em https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16

> Os programas de aprendizado de máquina não são neutros; as agendas de pesquisa e os conjuntos de dados com os quais trabalham frequentemente herdam crenças culturais dominantes sobre o mundo. Essas agendas de pesquisa refletem os incentivos e perspectivas daqueles que estão na posição privilegiada de desenvolver modelos de aprendizado de máquina e os dados nos quais eles dependem. A aceitação acrítica de suposições padrão inevitavelmente leva a um design discriminatório em sistemas algorítmicos, reproduzindo ideias que normalizam hierarquias sociais e legitimam a violência contra grupos marginalizados[300].

A questão relativa aos vieses dos dados já é grave o suficiente para não recomendar a utilização de *big data* e inteligência artificial para a predição de comportamentos criminosos, mas os problemas não se esgotam aí. Ferguson[301] questiona os limites éticos do policiamento preditivo, questionando se, da mesma forma que uma farmácia pode prever que um cliente provavelmente irá utilizar um cupom de desconto porque comprou um produto similar anteriormente, seria moralmente aceitável e juridicamente legítimo os órgãos estatais encarregados da persecução penal adotarem medidas restritivas de direito fundadas no fato de os algoritmos "preverem" que alguém iria vender drogas, por ter o sistema de inteligência artificial, por exemplo, classificado como "suspeito" o indivíduo a partir de suas postagens em redes sociais ou de registros de que essa pessoa comprou um número não usual de mini sacolas plásticas comumente utilizadas para a embalagem e venda de drogas.

Ainda que existam muitas iniciativas e discussões sobre a criminalização preditiva, sua implementação efetiva ainda é algo que somente ocorrerá no futuro. Entretanto, há atualmente inúmeras formas de utilização das modernas tecnologias de monitoramento e vigilância que estão em curso e que representam um enorme desafio ao estado de direito. De fato, as discussões sobre os limites do uso das novas tecnologias no âmbito criminal são urgentes, pois se ligam à própria definição dos limites do direito penal e do espaço de proteção que deve ser conferido ao indivíduo ante a atuação estatal. Assim, deve ser questionado, por exemplo, se tão-somente o estabelecimento de uma correlação forte entre um indivíduo e a ocorrência de um crime a partir da análise de dados agregados pode justificar a restrição a direitos fundamentais, ou qual o nível de proteção que deve ser conferido aos dados armazenados em um aparelho celular ou nos serviços de armazenamento de dados na nuvem.

---

[300] Tradução nossa. No original: "Machine learning programs are not neutral; research agendas and the data sets they work with often inherit dominant cultural beliefs about the world. These research agendas reflect the incentives and perspectives of those in the privileged position of developing machine learning models, and the data on which they rely. The uncritical acceptance of default assumptions inevitably leads to discriminatory design in algorithmic systems, reproducing ideas which normalize social hierarchies and legitimize violence against marginalized groups".

[301] FERGUSON. Andrew Guthrie. Op. Cit., p. 335

Por isso, a fim de se tentar criar bases para a construção de uma resposta para os limites do exercício do poder punitivo em um ambiente cada vez mais marcado pela utilização de dados pessoais compartilhados pelos indivíduos, é preciso compreender não só as formas modernas de *surveillance* e sua relação com o direito penal, mas também analisar a forma como a privacidade vem despontando como limite epistemológico à produção de provas em matéria criminal e como isso vem sendo tratado pela jurisprudência do STF.

4.1 SURVEILLANCE

O conceito de *surveillance* está ligado à ideia de vigilância. A expressão tem origem na palavra "surveille" do francês, que significa, em tradução literal, "observar" ou "fiscalizar", e talvez essa origem explique a existência de uma forte tendência de se pensar a *surveillance* como um fenômeno limitado à obtenção de dados acerca do objeto observado. A *surveillance*, porém, deve ser compreendida de forma mais ampla do que a mera observação e obtenção de dados, já que ela implica também um componente teleológico, uma finalidade com a qual ela é realizada. Neste sentido, afirma Lyon,[302] que *surveillance* são as operações e experiências de coleta, armazenamento e análise de informações pessoais para influenciar, conferir direitos ou gerenciar. No mesmo sentido, Julia Cohen[303] ressalta que a *surveillance* é uma atenção que se manifesta de maneira rotineira, sistemática, focada e feita com um propósito. Trata-se de uma forma de controle social que tem se espalhado rapidamente na atual organização social e que une governos, empresas e outras organizações sociais, constituindo na realidade um modo de governança, de organização da sociedade e de exercício do poder.

Apesar de comumente a *surveillance* ser identificada com a metáfora orwelliana do *Big Brother*, ligada à imagem de um governo central autoritário, o fato é que atualmente a surveillance se espalha por toda a sociedade e tem raízes profundas também na administração de países democráticos, com fundamentos teóricos que passam pelo panótico de Bentham e os aparatos de vigilância e disciplina de que trata Foucault. Não se cuida, portanto, de um projeto de poder centralizado e antidemocrático.

Por isso é que, na verdade, provavelmente a metáfora mais adequada para ilustrar o papel da surveillance na sociedade atual não seja a do Big Brother de Orwell, mas sim a de "O

[302] LYON, David. **The culture of surveillance.** p. 6

[303] COHEN, Julia. **Surveillance versus privacy: effects and implications.** in GRAY, David, HENDERSON, Stephen E., (orgs). **The Cambridge handbook of surveillance law.** New York: Cambridge University Press, 2017. p. 455-470.

processo", de Franz Kafka. A obra tem como protagonista Joseph K., que é detido sem que lhe seja informado o porquê. Ele tenta desesperada e insistentemente descobrir a razão, mas se depara com um sistema penal misterioso e insondável, no qual decisões vitais para ele são tomadas a partir de informações existentes em um dossiê cuja existência ele desconhecia e de cujo conteúdo ele sequer desconfia. Esse desequilíbrio nas relações entre o indivíduo e as instâncias de poder, agravado pela possibilidade de que decisões sejam tomadas a partir de dados que sequer são de conhecimento do interessado, acabou por se tornar uma perfeita alegoria da atual dinâmica de organização social, na qual o indivíduo não tem controle e nem mesmo ciência da utilização de seus dados e que é prevalente mesmo em estados democráticos.

É certo que governos autoritários (e as experiências históricas do nazismo, da União Soviética, da Alemanha Oriental e das diversas ditaduras latino-americanas demonstram isso muito claramente) sempre se valem de um aparato de vigilância para manter o controle de sua população. Entretanto, as sociedades democráticas também se utilizam da surveillance como forma de garantir uma maior eficiência e racionalidade na adoção das políticas públicas. Por isso, como afirma Kirstie Ball[304], mais do que um modelo típico de governos autoritários,

> A sociedade de vigilância (*surveillance society*) é melhor compreendida como o resultado de práticas organizacionais modernas, negócios, governo e militares do que como uma conspiração encoberta. A vigilância pode ser vista como um progresso em direção a uma administração eficiente, na visão de Max Weber, um benefício para o desenvolvimento do capitalismo ocidental e do moderno estado-nação[305]

Essa compreensão mais ampla de *surveillance* permite evitar duas grandes "armadilhas teóricas" sobre o tema: a primeira é pensar na surveillance como algo inerentemente ruim, produto de uma ação maligna de poderosos que pretendem controlar tudo e a todos; a segunda, é pensar na surveillance como um fenômeno da modernidade, produto exclusivo do desenvolvimento da tecnologia.

Quanto à primeira das questões, é de se ver que a moderna surveillance, feita com a participação ativa e voluntária dos usuários e que tem na iniciativa privada a mais importante fonte de recolhimento de informações pessoais, não é uma ação exclusivamente estatal e nem

---

[304] BALL, Kirsten *et al*. **A Report on the Surveillance Society For the Information Commissioner by the Surveillance Studies Network.** Disponível em https://www.personuvernd.is/media/frettir/surveillance_society_full_report_final.pdf

[305] Tradução livre. No original: "the surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy. Surveillance may be viewed as progress towards efficient administration, in Max Weber's view, a benefit for the development of Western capitalism and the modern nation-state."

tampouco pode ser compreendida como uma atividade que somente acarreta riscos, já que ela apresenta também inegáveis vantagens tanto para o indivíduo quanto para a coletividade.

A surveillance comercial, praticada primariamente pelas empresas de tecnologia, é parte de um modelo econômico que se especializou em identificar (ou inferir) os interesses dos consumidores para predizer o que, onde e o quanto eles estão dispostos a pagar para satisfazer tais necessidades. As sugestões personalizadas de filmes da Netflix ou de compras da Amazon, a partir das preferências do usuário, bem como a organização dos *feeds no Facebook* no *Twitter,* são exemplos de comodidades que tornam atrativos os serviços para os usuários. Por isso, o monitoramento constante pelas empresas de tecnologia das atividades do usuário na rede constitui uma forma de obtenção de informações que, a par de servirem de commodity para as empresas, também irão permitir uma melhor experiência para o usuário que, exatamente por essa razão, autoriza tranquilamente a cessão, uso, processamento e transferência de seus dados.

Assim, a atual lógica de organização do capitalismo, baseada na utilização, pelas empresas de *big data*, das informações pessoais mineradas dos seus usuários como instrumento de obtenção de mais-valia, transformando as experiências pessoais em fontes de lucro, não pode ser analisada de uma forma maniqueísta, já que ela apresenta, ao mesmo tempo, tanto vantagens quanto desvantagens. De fato, essa nova lógica, ao mesmo tempo em que seduz os usuários com as promessas de acesso ao fantástico mundo das novas tecnologias, a um custo que parece, à primeira vista, bem pouco significativo (a autorização de acesso e processamento dos dados pessoais), também aumenta de forma incomensurável a submissão e as possibilidades de controle daqueles que fornecem suas informações. Nesse ponto, vale lembrar que, como afirma Shoshana Zuboff[306], o capitalismo de vigilância é melhor descrito

> como um golpe impulsionado pelo mercado vindo de cima. Não é um golpe de estado no sentido clássico, mas sim um golpe de gens: uma derrubada do povo disfarçada como o cavalo de Tróia tecnológico que é o Grande Outro. Com a força de sua anexação da experiência humana, este golpe atinge concentrações exclusivas de conhecimento e poder que mantêm sua influência privilegiada sobre a divisão da aprendizagem na sociedade: a privatização do princípio central da ordem social no século XXI[307]

[306] ZUBOFF, Shoshana, **The age of surveillance capitalism. the fight for a human future at the new frontier of power.** New York:PublicAffairs, 2019. p. 513

[307] Tradução nossa. No original: "as a market-driven coup from above. It is not a coup d'état in the classic sense but rather a coup de gens: an overthrow of the people concealed as the technological Trojan horse that is Big Other. On the strength of its annexation of human experience, this coup achieves exclusive concentrations of knowledge and power that sustain privileged influence over the division of learning in society: the privatization of the central principle of social ordering in the twenty-first century".

Um aspecto que merece ser salientado e que demonstra bem a ambivalência desse modelo é que se por um lado as empresas de tecnologia conseguem obter lucro a partir de transações com os dados pessoais de seus usuários, por outro, é inegável que no atual modelo de negócio as empresas fornecem a eles conveniências e vantagens que, de outra forma, somente seriam acessíveis mediante cobrança pelo acesso ao serviço, o que fatalmente excluiria grande parte da população. Assim, por mais que tenha se tornado lugar comum a afirmação de que "se o serviço é de graça, o produto é você", o fato é que foi a partir desse modelo de negócio que se tornou possível a rápida expansão da internet e das novas tecnologias da informação e comunicação a um número gigantesco de usuários.

Da mesma forma, quando o enfoque passa a ser a atuação estatal, tem-se que a obtenção das informações está ligada também (especialmente nas sociedades democráticas) à busca por uma maior eficiência da atuação estatal. Aliás, como afirma John Gray[308], a surveillance em massa também serve a outros propósitos que não a acumulação de capital. Nas sociedades ocidentais, ela tem sido utilizada como instrumento do "liberalismo paternalista", que tenta influenciar as pessoas a tomarem decisões que ajudem a implementar o interesse público. Mesmo na China, aplicativos como o *Weibo* e o *WeChat* têm sido utilizados também para possibilitar a identificação das necessidades da população e melhor direcionar a atuação estatal.

Assim, também sob esse aspecto relacionado à atuação estatal, é inegável que, para além dos riscos à privacidade e à autonomia do indivíduo, a vigilância permite também ganhos. Com efeito, a existência de dados e informações relevantes permite racionalizar a atuação estatal na implementação de políticas públicas, melhorando seu alcance e sua efetividade. Os dados coletados permitem melhor planejamento e distribuição, possibilitando redução de gastos e aumento de resultados para a população.

Mesmo quando se tem em mente a surveillance voltada à obtenção de dados dos cidadãos para posterior utilização no campo da segurança pública, a razão que justifica a implementação de programas massivos de vigilância por câmeras de vídeo ou o monitoramento das redes sociais em busca de indicativos de ataques terroristas, por exemplo, é uma obtenção de maior eficiência na segurança cidadã. Aliás, especificamente no campo da segurança pública, é importante ressaltar que a existência de informações de inteligência que possam orientar as políticas de segurança é requisito essencial para que o Estado atue de forma a maximizar a sua eficiência na tutela do direito à segurança, dado que a

[308] GRAY, John. **Surveillance Capitalism Vs. The Surveillance State.** Noema Magazine, junho de 2020. Disponível em https://www.noemamag.com/surveillance-capitalism-vs-the-surveillance-state/

implementação de políticas que não sejam baseadas em dados concretos acaba por permitir uma atuação meramente ideológica, no mais das vezes fundada na cultura do medo[309].

No que diz respeito à visão de que a vigilância é um fenômeno moderno, surgido como o desenvolvimento tecnológico, cumpre notar que a surveillance, entendida como um processo que compreende a coleta, a análise e a utilização de informações, não surgiu com as novas tecnologias de informação e comunicação, mas na verdade é uma prática muito antiga, que sempre fez parte da socialização e da rotina institucional humana. É inegável, entretanto, que nos últimos 50 anos houve uma transformação social que modificou enormemente o modo de obtenção de informações, historicamente limitado pela capacidade dos sentidos humanos, especialmente da visão e da audição.

O desenvolvimento de novas tecnologias de comunicação e informação alterou as dinâmicas de poder e as relações pessoais a um ponto comparável às grandes transformações históricas, como a revolução industrial e a urbanização, por exemplo. Assim, apesar de nas sociedades humanas sempre terem existido dinâmicas de obtenção de informações, o impacto da revolução tecnológica marcou uma profunda alteração na forma como essa vigilância é feita, permitindo divisar uma classificação das formas de surveillance.

Para Gary T. Marx[310], a surveillance pode ser "não-estratégica", quando se refere unicamente à obtenção de dados que são rotineiros e facilmente apreendidos a partir de nossos instintos e sentidos, de forma não ordenada, a partir dos elementos disponíveis em nosso campo de percepção. Por outro lado, a surveillance se caracteriza como "estratégica", quando envolve a adoção de uma estratégia consciente dirigida à obtenção de informações.

A surveillance estratégica pode ser classificada de acordo com os métodos utilizados para se obter as informações, sendo denominada de "tradicional" quando se utiliza de métodos próprios das sociedades pré-industriais e que geram dados locais, compartimentalizados, cujo compartilhamento e análise demandam um grande esforço. Por seu turno, quando envolve o uso de tecnologia para extrair ou criar informações relacionadas

---

[309] Sobre a importância de dados na definição de políticas de segurança pública, ver ZILLI, Luís. **Mensurando a violência e o crime: potencialidades, vulnerabilidades e implicações para políticas de segurança pública**. Revista Brasileira de Segurança Pública. Vol. 12. 30-48, 2018. Disponível em https://www.researchgate.net/publication/330114490_Mensurando_a_violencia_e_o_crime_potencialidades_vulnerabilidades_e_implicacoes_para_politicas_de_seguranca_publica. Sobre a instrumentalização do medo na definição de políticas de segurança pública, ver PASTANA, Débora Regia. **A cultura do medo: reflexões sobre violência criminal, controle social e cidadania no Brasil.** São Paulo: editora Método, 2003.

[310] MARX, Gary. T. **"Yous papers, please": personal and professional encounters with surveillance.** in BALL, Kirstie, HAGGERTY, Kevin e LYON, David. **Routledge handbook of surveillance studies.** New York: Routledge, 2014

a contextos, indivíduos ou grupos, a doutrina[311] a denomina de *nova surveillance*. Essa nova surveillance é que constitui elemento central da atual organização social. Em comparação à surveillance tradicional, ela é mais extensa, mais intensa e frequentemente envolve múltiplos parâmetros, sendo que a coleta de informações é normalmente feita de forma automática, sem intervenção humana direta.

Essa nova forma de surveillance (que daqui em diante será referida apenas como surveillance) é um aspecto central do capitalismo informacional, uma nova lógica de acumulação que procura prever e modificar o comportamento humano como forma de gerar receitas e controle de mercado.[312]

Vale notar que essa forma de utilização das novas tecnologias pelos órgãos estatais, na qual a busca pela garantia de segurança passa pela utilização de dados coletados por empresas e pela ampliação do controle de dados disponíveis na internet, tende a se acentuar ainda mais com o aumento da conectividade e a implementação de novas tecnologias como a telefonia 5G e a internet das coisas, que permitirão a troca de dados entre diversos dispositivos conectados pela rede mundial sem o conhecimento dos usuários. Tecnologias como o monitoramento em tempo real dos GPS nos celulares, a georeferenciação utilizada por sites na internet, os televisores e outros aparelhos domésticos que captam conversas das pessoas no ambiente, e as câmeras de vigilância com reconhecimento biométrico, cada vez mais passarão a constituir algo corriqueiro, fornecendo possibilidades de vigilância e controle que até bem pouco somente eram pensadas em obras de ficção científica.

Cria-se, assim, um gigantesco volume de dados compartilhados voluntariamente pelos usuários com as empresas, que passa a constituir um valioso banco de dados para a obtenção de informações potencialmente relevantes para a investigação e prevenção de infrações penais. Tais informações coletadas primariamente pelas empresas estão sujeitas à utilização secundária pelo Estado, já que podem ser obtidas por meio de requisições das autoridades encarregadas da persecução penal às empresas detentoras dos dados.

A vigilância digital passa a ser feita pelas agências governamentais a partir de dados já colhidos normalmente pelas empresas privadas para suas operações, de modo que, como afirma David Lyon[313], a surveillance digital ou *dataveillance* é um drama do qual participam

---

[311] MARX, Gary T. **Whats's new about new surveillance'? Classifying for change and continuity.** in Hier, Sean e Greenberg, Josh. **The surveillance studies reader.** New York: McGraw-Hill. 2007, pp. 83-95.

[312] ZUBOFF, Shoshana. ***Big other:* capitalismo de vigilância e perspectivas para uma civilização de informação.** in BRUNO, Fernanda et al. **Tecnopolíticas da vigilância. perspectivas da margem.** São Paulo: Boitempo, 2018. p. 18

[313] LYON, David. **Surveillance**, **Snowden, and Big Data: Capacities, consequences, critique.** Big Data & Society – Jul-Dez 2014. Disponível em http://journals.sagepub.com/doi/abs/10.1177/2053951714541861

três atores: as agências governamentais, as empresas de tecnologia e, mesmo que involuntariamente, os usuários finais.

O que torna possível a existência desse extenso e intenso programa de vigilância e controle, unindo os três atores, são os algoritmos, os códigos de programação que selecionam, extraem, separam e possibilitam a utilização das informações prestadas pelos usuários. Para as empresas de tecnologia, essas informações são importantes para possibilitar publicidade dirigida ou contextual, além de possibilitar o oferecimento de soluções personalizadas, aumentando a conveniência e facilidade da utilização e melhorando a experiência para os usuários. Para as agências governamentais, trata-se de um enorme banco de dados à disposição para a obtenção de dados de inteligência que podem ser utilizados para vigilância e controle. Para os usuários, trata-se, no mais das vezes, do preço a pagar pelo acesso aos serviços. E o que os usuários recebem em troca do fornecimento de seus dados, é o "incrível poder da internet de mantê-los conectados, divertidos, entretidos, abastecidos, atualizados, encorajados e informados"[314].

No presente trabalho, focaremos nesta nova modalidade de surveillance, uma vigilância estratégica que utiliza de instrumentos tecnológicos para coletar ou criar dados pessoais que podem ser utilizados para gerar informação e conhecimento. No contexto de segurança pública, a surveillance estratégica pode ser entendida como o monitoramento sistemático de pessoas ou grupos por meio de sistemas de informação, com vistas a regular ou determinar o seu comportamento[315]. As modernas tecnologias de informação e comunicação permitem que os dados pessoais compartilhados pelos usuários e que são massivamente coletados, agregados, processados e disseminados pelas empresas de tecnologia possam ser apropriados e utilizados pelas autoridades encarregadas da persecução penal.

Assim compreendida, a surveillance se aproxima do conceito de atividade de inteligência para aplicação da lei penal, que, nos termos do disposto no art. 2ª do Decreto 4.376/2002, é "atividade de obtenção e análise de dados e informações e de produção e difusão de conhecimentos, dentro e fora do território nacional, relativos a fatos e situações de imediata ou potencial influência sobre o processo decisório, a ação governamental, a salvaguarda e a segurança da sociedade e do Estado". A inteligência em segurança pública, portanto, é uma atividade ligada à análise de informações brutas retiradas da realidade, a

[314] Lyon, David. **The culture of surveillance.** p. 4

[315] FERGUSON. ANdrew Guthrie. **Big Data Surveillance: the Convergence of Big Data and Law Enforcement.** in GRAY, David, HENDERSON, Stephen E., (orgs). **The Cambridge handbook of surveillance law.** New York: Cambridge University Press, 2017. p. 171- 197.

partir de inúmeras fontes, tanto abertas como fechadas, com a finalidade de orientar a tomada de decisões por parte dos responsáveis pela implementação das políticas de segurança.

4.2 VIGILÂNCIA, INTELIGÊNCIA POLICIAL E A EXPANSÃO DO DIREITO PENAL

Tradicionalmente, há uma diferença marcante entre a atividade de inteligência e a de segurança pública, decorrente da forma como o ordenamento jurídico trata as informações de inteligência e aquelas destinadas a serem utilizadas como provas na persecução penal. De fato, uma vez que os informes de inteligência se destinam unicamente a possibilitar decisões estratégicas, especialmente dos órgãos vinculados ao sistema de inteligência encarregados da segurança do Estado ou da defesa nacional, sua produção e utilização não estão submetidas ao mesmo rigor formal e material exigidos para a produção de elementos que servirão como prova em processos criminais, que devem cumprir as regras legais que estipulam limites à sua produção e utilização, bem como devem ser submetidas ao crivo das partes, a quem deve ser assegurado o contraditório, ainda que diferido[316].

O aumento da capacidade de obtenção de dados por parte das autoridades encarregadas da persecução penal, especialmente pela utilização de ferramentas de inteligência artificial, *big data* e do acesso a dados obtidos e tratados pelas empresas de tecnologias, acabaram por abalar essa diferenciação, dado que aspectos da intimidade e da privacidade dos cidadãos que anteriormente somente eram acessíveis por meio de intensivas e custosas atividades de inteligência passaram a ser facilmente obtíveis através de meios à disposição das agências ligadas à segurança pública.

Cada vez mais as atividades de persecução penal e de inteligência destinadas à segurança nacional ou defesa do Estado passaram a se valer de métodos muito similares de obtenção de informações. A difusão das novas tecnologias de vigilância, aliada à busca pelo aumento da eficiência e eficácia das ações estatais voltadas à segurança pública e à persecução penal, estão fazendo com que essa atividade estatal de inteligência se torne, pelo menos no que concerne aos métodos e meios de obtenção de informações, indistinta da atividade de obtenção de provas para a persecução penal, tornando o policiamento e

[316] CF. MELLADO, Jose Maria Asencio. **Los informes de inteligencia policiales. su influencia en los principios esenciales del proceso penal** *in* PEREIRA, Flavio Cardoso (org.) **Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo**. Brasilia, DF : Gazeta Juridica, 2016.

especialmente a investigação de crimes feita pela polícia judiciária bastante similares à espionagem feita pelas agências de inteligência.

Em um mundo predominantemente analógico, a obtenção de dados dependia da utilização de muitos recursos humanos e materiais, o que na prática inviabilizava sua utilização rotineira pela polícia. Assim, por exemplo, caso as autoridades quisessem obter informações sobre a rotina diária de alguém que fosse alvo de uma investigação, deveriam mobilizar agentes que pudessem de alguma forma estar fisicamente próximos do investigado, para que fizessem um monitoramento constante e encoberto. Ademais, para que as informações pudessem ter validade como prova em um processo judicial, sempre que técnicas mais invasivas fossem utilizadas, elas deveriam ter prévia autorização judicial. Por todas essas circunstâncias, as polícias praticamente não se valiam dessas técnicas investigativas e as informações mais sensíveis somente eram coletadas por agências de inteligência que, por força da própria natureza da sua atividade, as utilizariam unicamente como elementos para possibilitar a tomada de decisões.

Em um mundo digital extremamente interconectado, essas informações passaram a estar facilmente acessíveis a partir da utilização das tecnologias à disposição das polícias, ao alcance de um clique. As polícias passaram a utilizar cotidianamente as mesmas técnicas investigativas das agências de inteligência, que passaram a ser tecnologicamente possíveis e economicamente acessíveis.

A ampliação da surveillance baseada nas novas tecnologias vem progressivamente levando a uma interpenetração da coleta e análise de dados nas atividades de inteligência e de persecução penal, gerando o que Ales Zavrsnik[317] chama de "androginia de segurança", modelo em que as forças militares passam a ser utilizadas para fazer policiamento interno e a polícia assume cada vez mais um papel paramilitar, passando a atuar orientada para a prevenção, com base em informações de inteligência, ao passo que as agências de inteligência, premidas pelas chamadas "ameaças internas" e pelo receio de ataques terroristas, se tornam cada vez mais comprometidas com medidas relacionadas à manutenção da segurança pública. Para ele, no plano internacional, cada vez mais as atividades de persecução penal e inteligência externa têm se sobreposto, em termos institucionais, operativos, tecnológicos e espaciais, e isso se intensificou muito nas duas últimas décadas.

[317] ZAVRŠNIK, Ales. **Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?** Journal of Contemporary European Research. vol. 9, 2013. pp. 181-202. disponível em https://www.jcer.net/index.php/jcer/article/view/452

O ofuscamento dos limites entre as atividades de inteligência e de persecução penal levou a uma sobreposição de funções e atividades, que pode ser evidenciado, no campo institucional, pelo surgimento de agências de cooperação e troca de informações, especialmente no plano internacional, com polícias, ministérios públicos e órgãos judiciários criando extensas redes globais de cooperação e troca de informações por canais informais e não diplomáticos, do que a Interpol[318], o El Paccto[319] e a Eurojust[320] são exemplos marcantes.

No plano espacial, a sobreposição se evidencia pela atuação de entes encarregados da persecução penal em crimes transfronteiriços e em casos de ameaças externas, ao passo que as agências de inteligência passaram a atuar também sobre as chamadas "ameaças internas" ou "terrorismo doméstico".

O entrelaçamento das atividades de inteligência e persecução penal se evidencia ainda, e sobretudo, pela ampla difusão da noção de que o policiamento interno voltado à segurança cidadã deve ser feito a partir da coleta de dados de inteligência, o que levou à utilização, pelas polícias judiciárias e demais entes encarregados da investigação criminal, de métodos de investigação invasivos, próprios das entidades de inteligência e segurança externa, que incluem, entre outros meios, a utilização de *trojans* (programas instalados sub-repticiamente e que executam ações em um computador criando uma porta para uma possível invasão sem a autorização do usuário, a fim de obter os dados da máquina) ou a vídeo surveillance com reconhecimento biométrico ou de placas de veículos.

Essa sobreposição de atuações entre segurança e inteligência torna ainda mais delicado o balanceamento entre privacidade e segurança pública, pois a admissão de dados de inteligência no processo penal, como prova a ser utilizada contra um indivíduo, especialmente em um contexto em que esses dados foram compartilhados com terceiros (geralmente

[318] International Criminal Police Organization (Interpol) é uma organização intergovernamental que conta atualmente com 195 países membros e que visa a possibilitar a cooperação entre as polícias nacionais de seus membros, possibilitando o compartilhamento de dados de crimes e criminosos, bem como oferecendo suporte técnico e operacional.

[319] Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado (Programa de Assistência Europa América Latina contra o Crime Organizado Transnacional), é um programa de cooperação internacional financiado pela União Europeia que busca contribuir para a segurança e a justiça na América Latina, apoiando o combate ao crime organizado transnacional, abordando a cadeia penal de uma perspectiva abrangente por meio de sua atuação em três componentes: polícia, justiça, prisão. Trata-se de um programa de assistência técnica entre a União Europeia e a América Latina que fomenta o intercâmbio de experiências e boas práticas, facilitando a troca de informações e a cooperação internacional em matéria judiciária.

[320] Agência da União Europeia para a Cooperação em Justiça Criminal, que funciona como um centro único no qual as autoridades judiciárias de cada um dos países membros trabalham em estreita colaboração para combater o crime organizado transfronteiriço grave. Seu papel é coordenar o trabalho das autoridades nacionais dos Estados-Membros da UE, bem como de Estados terceiros participantes na investigação e repressão do crime transnacional.

empresas de tecnologia) para outras finalidades, levanta questões acerca dos riscos às liberdades civis e aos limites do direito penal.

Na realidade, o próprio balanceamento entre os poderes estatais relativos à persecução penal e as liberdades constitucionalmente conferidas aos cidadãos acaba sendo profundamente alterado por esta interpenetração de dados e informes de inteligência no processo criminal, o que se torna ainda mais preocupante quando se tem em mente o fato de que as informações produzidas a partir das novas tecnologias tendem a ser recebidas sob um olhar tecnodeterminista, que confere a elas uma aura de "prova científica" incontestável, contra a qual há poucas ou nenhuma possibilidade de defesa.

Um bom exemplo disso são os laudos de reconhecimento facial feito a partir de dados biométricos analisados por algoritmos de inteligência artificial, que tendem a ser aceitos como verdadeiros e exatos, mesmo a despeito dos incontáveis exemplos das falhas e vieses que este tipo de tecnologia traz consigo; ou o exame de *logs* de acesso a sites ou histórico de chamadas e de localização dos aparelhos celulares utilizados pelos investigados, que tampouco são elementos que admitem muita margem para qualquer contestação.

Nestas condições, tem-se que a expansão das novas tecnologias e a moderna surveillance que ela proporciona, com o baixo custo da obtenção de informações de inteligência e dados pessoais que podem ser utilizados para instruir processos criminais, ajudam a compor um ambiente em que até mesmo as bases sobre as quais tradicionalmente se estruturou o direito penal passam a ser afetadas.

Em praticamente todos os ordenamentos jurídicos atuais se adota um modelo de direito penal marcado fundamentalmente pela limitação do poder punitivo estatal, em que são estatuídas uma série de garantias aos cidadãos contra o Estado. Esse conjunto de direitos e garantias forma o chamado modelo de "direito penal clássico", cunhado a partir da tradição jurídica do iluminismo e do liberalismo[321].

O modelo de Estado construído a partir das ideias iluministas é o Estado de direito, com a submissão de todos (inclusive – e principalmente – do governante) às leis, tendo como tônica a afirmação dos direitos do homem e do cidadão e a limitação do poder estatal à garantia desses direitos, especialmente aqueles relacionados à liberdade individual e à propriedade. A persecução penal, assim, tem como tônica a adoção de uma postura essencialmente cética quanto à acusação feita contra o indivíduo, que é retratada no estado de inocência, que simultaneamente é uma regra de tratamento (não se admite que o réu seja

321 Cf. FERRAJOLI, Luigi. **Direito e razão:** teoria do garantismo penal.3ª. ed. São Paulo: RT, 2010. P. 37 e SS.

tratado como culpado) e uma regra de distribuição do ônus da prova (cabe ao estado acusador o dever de apresentar elementos que permitam concluir, acima de uma dúvida razoável, que o réu efetivamente praticou as condutas que lhe foram imputadas).

Como consequência, em face do estado-acusação, o estado juiz comprometido com a tutela dos direitos fundamentais do cidadão deve assumir sempre uma postura cética, de modo que a acusação tenha que superar estandartes probatórios mínimos caso queira obter a condenação do réu.

O Estado de Direito, portanto, é um modelo de Estado vocacionado à limitação do poder punitivo e à proteção do indivíduo contra a arbitrariedade, construído historicamente a partir do ideário iluminista que enxerga o crime como uma violação às regras estatuídas de acordo com o contrato social, que consagrou a legalidade como um freio ao poder punitivo de reis e nobres, que buscou estabelecer limites ao arbítrio judicial e que se contrapôs ao uso da tortura como meio de investigação e da pena de morte como sanção.

Ressalte-se que foi principalmente a partir do movimento político e filosófico do Iluminismo que o direito penal começou a ganhar contornos científicos, com o delito perdendo suas bases religiosas e passando a ser analisado sob uma perspectiva racional, utilitarista, onde a pena passa a ser vista não mais como um meio de expiação do pecado, mas como uma forma de se prevenir a prática de crimes, configurando um mal menor. Por isso que, como afirma Ferrajoli[322],

> Desde Grozio, Hobbes, Locke, Puffendorf y Thomasius hasta Montesquieu, Beccaria, Voltaire, Filangieri, Bentham y Pagano, todo el pensamiento penal reformador está de acuerdo en considerar que las aflicciones penales son precios necesarios para impedir daños mayores a los ciudadanos, y no constituyen homenajes gratuitos a la ética o a la religión o al sentimiento de venganza.

Em linhas gerais, essas foram as principais ideias que moldaram o modelo garantista do direito penal que se perpetuou até nossos dias. Pode-se afirmar, assim, que desde a Ilustração vem sendo desenvolvida uma dogmática penal voltada à limitação do poder punitivo e ao afastamento da arbitrariedade na aplicação das penas. Por isso é que Ferrajoli afirma que, no modelo garantista, as "regras do jogo fundamental do direito penal" são produto do pensamento iluminista[323], onde foram concebidas como princípios políticos, morais ou naturais de limitação do poder penal "absoluto", tendo sido, em maior ou menor

[322] FERRAJOLI, Luigi. **El Derecho Penal Mínimo.** In. RAMÍREZ, Juan Bustos (dir.) Prevención y teoría de la pena. Santiago de Chile: Editorial Jurídica Conosur, 1995. p. 33

[323] FERRAJOLI, Luigi. **Direito e razão. Teoria do garantismo penal.** P. 92

graus, incorporados a todas as constituições e codificações dos ordenamentos desenvolvidos, convertendo-se, assim, em preceitos fundamentais do moderno Estado de Direito.

O modelo garantista, assim, é o conteúdo típico do direito penal da Ilustração, que Hassemer chama de direito penal clássico[324], e que tem como principal característica o fato de se desenvolver a partir de uma estrutura de intervenção sujeita a limites estritos impostos pela lei. Vale ressaltar, ainda, que o modelo garantista de direito penal não tem a pretensão ou a finalidade de descrever um modelo existente na realidade fenomênica, mas configura um modelo ideal, uma meta, uma ideia-guia que confere um horizonte de sentido que guia a direção para a qual deve caminhar a evolução do direito penal. Por isso, como afirma Bobbio, "o garantismo é um modelo ideal ao qual a realidade pode mais ou menos se aproximar. Como modelo representa uma meta que permanece tal mesmo quando não é alcançada, e não pode ser nunca, de todo, alcançada"[325].

Trata-se, assim, de um modelo de Estado de Direito que, para Ferrajoli, deve ser utilizado para aferir o grau de racionalidade e de certeza existente em um dado sistema penal, de modo que, a partir dele, é possível avaliar-se as instituições e o ordenamento de um sistema concreto a fim de aferir-se uma maior tendência ao direito penal mínimo (mais aproximado do modelo garantista) ou ao direito penal máximo (mais aproximado a um modelo autoritário).

Mesmo a despeito de historicamente esse modelo teórico ter sido clara e frontalmente desrespeitado em vários momentos no correr do século XX (do que as experiências do nazismo, do fascismo, do comunismo e das diversas ditaduras na América latina fornecem o exemplo mais eloquente) e mesmo no século XXI (vide a "guerra ao terror" em escala mundial instaurada após os eventos do 11 de setembro, os programas de vigilância revelados por Edward Snowden e a tendência cada vez mais forte de as políticas de segurança pública se utilizarem de dados pessoais), o modelo garantista ainda é a base sobre a qual se estrutura a maior parte da produção teórica em direito penal, e mesmo aqueles que o criticam

---

[324] Cabe fazer uma breve observação acerca da denominação aqui utilizada. É que na doutrina penal é usual que este modelo de direito penal cunhado a partir do ideário iluminista seja chamado de direito penal "moderno", em alusão à sua contemporaneidade ou em razão do fato de que ele representou a ruptura com o modelo do Antigo Regime. Entretanto, no debate penal atual, em que o modelo penal garantista tornou-se o paradigma das civilizações ocidentais e onde o debate penal está centrado exatamente na necessidade de superar ou pelo menos ajustar tal modelo, não mais parece adequado denominar-se o modelo iluminista de "moderno". Por isso é que Hassemer propôs a alteração desta terminologia, de modo que esse modelo do Iluminismo passasse a receber a denominação de direito penal clássico, reservando-se o termo "moderno" para designar o direito penal direito da atualidade. Sobre essa questão, ver MARTIN, Luis Gracia. **A modernização do direito penal como realização do postulado do Estado de Direito (social e democrático).** Revista Brasileira de Ciências Criminais. Nº 88, São Paulo: ed. Revista dos Tribunais, 2011

[325] BOBBIO, Norberto. **Prefácio à 1a edição italiana de Direito e razão.** p. 9

reconhecem não ser possível prescindir dos ganhos que ele trouxe para a contenção do arbítrio no exercício do *jus puniendi.*

A influência destes ideais sobre os sistemas penais configura uma conquista da humanidade, e se expressa sob a forma dos mais importantes fundamentos do sistema jurídico-penal. Entretanto, ainda que sigam amplamente aceitas as noções e ideias cunhadas sobre bases iluministas, de que o processo penal é um instrumento mediante o qual se determina a realidade dos fatos imputados ao réu e se aplica o direito objetivo, e de que o direito penal é um instrumento de proteção das condições básicas de convivência social, pela proibição de certos comportamentos que representem risco a essas condições, passamos atualmente por um momento em que, por diversos fatores, o direito penal vem se expandindo para alcançar uma função social muito distante daquela pensada na Ilustração.

Em obra que já se tornou referência sobre o tema, Silva Sanchez[326] aponta como principais causas da expansão do direito penal a aparição de novos bens jurídicos (como a confiança no mercado de capitais, a tutela das relações de consumo ou os direitos à privacidade digital, por exemplo); e a revalorização de outros anteriormente existentes, decorrente de novas realidades ou da deterioração de realidades tradicionalmente abundantes (como os recursos ambientais); o surgimento de novos riscos de procedência humana que se tornam estruturais à sociedade; a institucionalização da distribuição de riscos para toda a sociedade; a sensação social de segurança disseminada entre os membros da sociedade, acompanhada pela perda de referências valorativas e pela crescente exploração pela mídia de uma elevadíssima "sensibilidade ao risco"; a configuração de uma sociedade formada precipuamente por indivíduos em posições passivas (consumidor, usuário de serviços etc.), que são especialmente vulneráveis ao aumento do espaço de risco permitido; o descrédito de outras instâncias de proteção, como a moral, o direito civil ou o administrativo; uma certa atitude política dos setores progressistas e de grupos de pressão organizados, que reclamam uma firme atuação do direito penal do "combate" à criminalidade dos poderosos e dos violadores dos direitos fundamentais e a identificação da maioria da população com a vítima dos delitos, que leva à perda da visão do direito penal como meio de defesa do acusado, acentuando a necessidade de defesa das vítimas através do direito penal.

Em uma contundente crítica, Diez Ripollés[327] argumenta que a tese de Silva Sanchez peca por misturar dois fenômenos reais, mas que não só têm causas diferentes, mas também se

---

326 SILVA SANCHEZ, Jesus-Maria. **A expansão do Direito Penal** . P. 32 e ss.

327 DÍEZ RIPOLLÉS, José Luis. **El nuevo modelo penal de la seguridad ciudadana.** Revista Electrónica de Ciencia Penal y Criminología. 2004, núm. 06-03, p. 07. Disponível em http://criminet.ugr.es/recpc http://criminet.ugr.es/recpc.

movem em direções opostas: por um lado, a "modernização" do direito penal, que leva à sua incursão sobre novas modalidades de criminalidade socioeconômica, praticada principalmente pelos "poderosos"; por outro lado, há o fenômeno da "segurança cidadã", que leva ao aumento do rigor contra a criminalidade clássica, com aumento de penas e redução de garantias processuais e que tem nos marginalizados e excluídos o seu público-alvo preferencial. Para Ripollés, esses dois fenômenos, embora efetivamente reflitam uma expansão do direito penal, respondem a causas e a exigências ideológicas diversas, de modo que é incorreto analisá-los como se fossem parte de um mesmo movimento expansivo.

A utilização do direito penal como meio de gestão de riscos reflete uma abordagem precaucionária, que decorre de dois fenômenos distintos: a) o movimento de modernização para que o direito penal passe a tratar de temas anteriormente só destinados ao direito administrativo ou civil (como o direito penal ambiental, os crimes econômicos e cibernéticos, por exemplo) e b) o crescimento da sensação social de medo, que reclama o endurecimento de penas, a redução de garantias processuais e a antecipação da consumação para um momento anterior ao da produção da lesão (crimes de mera conduta e de perigo abstrato). Ambos os fenômenos que levam à expansão do direito penal guardam íntima relação com a intensiva utilização das novas tecnologias de informação e comunicação, em especial a internet, o *big data* e a inteligência artificial.

De fato, tanto a expansão fundada nos movimentos de lei e ordem quanto a expansão fundada na chamada "modernização" do direito penal se valem das novas tecnologias como instrumento privilegiado de atuação, sendo certo que, ainda que respondam a causas diversas, esse movimento por mais direito penal é decorrente de um conjunto de fatores sociais em grande medida ligados à tentativa de satisfazer a busca pelo controle de riscos sociais e de aplacar os temores a eles ligados, que geram fortes efeitos no campo da política criminal.

Para Díez Ripollés[328] esses fatores sociais podem ser agrupados em três blocos:

a) a generalização dos novos riscos artificiais, decorrentes de uma nova estruturação da sociedade e da utilização de novas tecnologias em diversos âmbitos sociais;
b) a inter-relação dos riscos sociais, que cria uma extensa rede de contatos que torna virtualmente impossível determinar-se a responsabilidade pelos riscos; e,
c) a existência de um exagerado sentimento de insegurança, resultado da combinação da intensa cobertura midiática da criminalidade, aliada à acelerada modificação das

328 DÍEZ RIPOLLÉS, José Luis**. De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado.** Revista Electrónica de Ciencia Penal y Criminología. 2005, núm. 07-01, p. 04. disponível em http://criminet.ugr.es/recpc http://criminet.ugr.es/recpc.

relações e valores sociais, com a cada vez maior proeminência de um individualismo exacerbado e a redução da solidariedade.

Esses fatores parecem estar em grande medida relacionados à configuração de uma sociedade pós-industrial, a sociedade da informação, em que a evolução das relações sociais chegou a um ponto tal que suas consequências acabaram por infirmar as bases sobre as quais a sociedade se estruturava, com a ampliação e disseminação do risco de tal forma que se inaugura uma nova etapa na evolução social. Trata-se de um momento histórico em que a evolução das condições de produção típicas da sociedade industrial modificou a estrutura de organização da sociedade e do Estado e acaba por também mudar a forma de percepção social do papel do direito penal. Nas palavras de Silva Sanchez[329],

> Seja como for, o certo é que a criminalidade organizada (narcotráfico, terrorismo, pornografia), a criminalidade das empresas (delitos fiscais, contra o meio ambiente, contra as relações de consumo – saúde e interesses econômicos), a corrupção político-administrativa ou o abuso de poder e, inclusive, a violência conjugal do denominado "tirano doméstico" e o acosso sexual aparecem no primeiro plano da discussão social sobre o delito. E a nova política criminal intervencionista e expansiva recebe as boas-vindas de muitos setores sociais antes reticentes ao Direito Penal, que agora acolhem como uma espécie de reação contra a criminalidade dos poderosos

Em uma sociedade em que as ameaças decorrentes das atividades humanas assumem papel preponderante, obviamente o papel reservado ao direito penal, mais poderoso instrumento social para a motivação de comportamentos, sai de sua órbita original (isto é, daquela que lhe foi reservada segundo a concepção clássica do modelo garantista) e passa a cada vez mais gravitar em torno da gestão de riscos. A expansão do direito penal, assim, não pode ser entendida unicamente como produto de manipulação ideológica por parte dos poderes políticos, que fariam uso meramente simbólico do aparelho repressor do Estado. Na verdade, força é reconhecer que existe uma série de novas realidades sociais que empurram o direito penal rumo à ampliação de seu âmbito de aplicação para áreas antes reservadas apenas a outras instâncias de controle social.

A preponderância dos riscos e perigos[330] na sociedade contemporânea faz com que a forma de proteção dos bens jurídicos pelo direito penal não mais se encaixe nos rígidos

---

329 SILVA SANCHEZ, Jesus-Maria. **A expansão do Direito Penal** . Pp. 68-69

330 Luhmann distingue entre riscos e perigos a partir da ideia de causalidade. Riscos seriam os danos futuros decorrentes de uma decisão, ao passo que perigos seriam os danos futuros decorrentes de fatores externos. Assim, os riscos seriam os danos futuros decorrentes de uma decisão do indivíduo, ao passo que os perigos seriam os danos futuros decorrentes de causas externas. Cf. LUHMANN, Niklas. **El concepto de riesgo**

padrões do modelo do direito penal clássico. Isso porque, numa organização social em que o risco passou a ser anônimo e onipresente, a política criminal passa a incluir também a tutela de bens jurídicos de natureza substancialmente diversa daquela dos bens individuais que moldaram o modelo de direito penal clássico e o faz de modo formalmente diferente também. Esvaem-se algumas das garantias fundamentais construídas ao longo do desenvolvimento da doutrina penal fundada no modelo garantista.

Uma importante parcela da doutrina penal tem se contraposto à expansão do direito penal, afirmando que o direito penal não pode nem deve ser utilizado como instrumento de gestão de riscos, sob pena de se fazer tábula rasa dos princípios garantistas. Os principais expoentes dessa corrente são professores alemães que integram a chamada "Escola de Frankfurt". Sob esta denominação, como bem nota Feijoo Sanchez[331], são incluídos autores abolicionistas, como Lüderssen e Albrecht, juntamente com autores reducionistas ou minimalistas, como Hassemer, Naucke, Prittwitz e Herzog, o que gera dúvidas quanto à efetiva existência de uma "escola" no sentido de um movimento ou de uma orientação definida. Entretanto, o termo se consolidou como forma de referência a autores que têm em comum uma visão extremamente restritiva do direito penal. Prittwitz expressamente admite a existência da escola de Frankfurt, afirmando que

> (...) o que a conforma é o contorno específico que adota sua crítica ao direito penal – o ceticismo ante sua capacidade de resposta, a recordação constante de seu potencial de terror e abuso, afirmando ao mesmo tempo o domínio incondicionado do direito em seu interior- onde cada um de seus membros coloca o acento tônico, importa tão pouco o fato de que tais críticas não se encontram apenas em Frankfurt".[332]

Para estes autores, os novos riscos sociais devem ser objeto de outros instrumentos de ação de controle, que, por não ter o potencial gravoso do direito penal, possam ter garantias e hipóteses de aplicação flexibilizadas. Nesse aspecto, Hassemer[333] propõe a redução do direito penal a um direito penal nuclear, restrito à tutela de bens jurídicos individuais ou, no máximo, de bens jurídicos coletivos que tenham como substrato um bem individual lesionado pelo crime e, para os novos riscos, propõe o que ele chama de "direito de intervenção", um espaço situado entre o direito penal e o direto das contravenções, entre o direito civil e o direito

---

in BERIAIN, Josetxo. (comp.) **Las consecuencias perversas de la modernidad. Modenidad, contingencia y riesgo** Barcelona: Anthropos, 1996, p. 144.

331 Cf. FEIJOO SANCHEZ, Bernardo. **Sobre a "administrativização" do Direito Penal na "sociedade do risco**". Notas sobre a política criminal no início do século XXI. Revista Liberdades. Nº 7, maio-agosto 2011. p. 26 nota 14.

332 APUD FEIJOO SANCHEZ. Op. Cit. P. 26

333 Cf. ROXIN, Claus. **Derecho Penal. Parte general.** P. 61

administrativo, onde as garantias e os procedimentos serão menos exigentes do que os do direito penal, mas em contrapartida as sanções que ele aplicará aos indivíduos serão proporcionalmente menos intensas.

Vale notar, entretanto, que o próprio Hassemer reconhece que "atualmente, uma teoria como essa não encontra mais uma conjuntura favorável"[334], pois esbarra na onda expansiva que encontra no direito penal canal privilegiado de controle social, de modo que é possível afirmar que a proposta de Hassemer de criação de um novo campo de controle social, diferente do direito penal (que ele denomina de direito de intervenção) é apenas mais uma proposta que, juntamente com outras como a do modelo de direito penal orientado para a ressocialização ou a do modelo da justiça restaurativa, acabam ocupando um lugar apenas marginal no sistema punitivo e nessa trilha expansiva percorrida pelo direito penal. Atualmente, assim, aparecem como relevantes dois modelos diferentes de direito penal, que frequentemente entram em colisão: o clássico, garantista, e o da sociedade de risco.

No novo modelo, o da sociedade de risco, a política criminal se caracteriza por quatro traços marcantes[335]:

1) Uma expressiva ampliação do âmbito social da aplicação da intervenção penal, que passa a atuar sobre novas realidades sociais problemáticas ou sobre realidades cuja vulnerabilidade tenha aumentado, como o meio ambiente, a proteção ao consumidor, a proteção ante novos riscos tecnológicos (nucleares, genéticos, da tecnologia da informação etc) e sócio-econômicos, em especial aqueles ligados à criminalidade organizada (v.g. o tráfico de drogas, de armas e de pessoas);

2) uma mudança de orientação da política criminal, que passa a mirar as atividades dos setores poderosos da sociedade, tradicionalmente excluídos do campo de atuação seletiva do direito penal. A ampliação do objeto da tutela penal aos novos riscos sociais muda esse enfoque, já que esses grupos influentes e poderosos são os únicos capazes de desenvolver e controlar as atividades geradoras ou potencializadoras dos novos riscos;

3) a ideia de que o direito penal é a mais eficaz forma de controle social, levando à sua proeminência sobre as outras formas de intervenção, como a moral, a religião ou a família, e mesmo sobre outras abordagens jurídicas, como a do direito civil e a do direito administrativo. Com isso, coloca-se seriamente em xeque o princípio da intervenção mínima, em especial no que diz respeito à subsidiariedade;

---

334 HASSEMER, Winfried. **Linhas gerais de uma teoria pessoal do bem jurídico.** P. 24.

335 Cf. DIÉZ RIPOLLÉS. José Luis. **De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado.** Revista Electrónica de Ciencia Penal y Criminología. Vol. 07-01, 2005. Disponível em <http://criminet.ugr.es/recpc/07/recpc07-01.pdf>

4) as necessidades de acomodação dos institutos do direito penal e do direito processual penal a essas novas formas de criminalidade, que apresentam uma série de dificuldades à utilização do direito penal garantista, em razão das dificuldades na delimitação do campo do risco permitido e na individualização das condutas. Além disso, essa nova criminalidade se vale de meios de atuação substancialmente diversos daqueles utilizados pela criminalidade clássica, o que torna necessária não só a existência de novas técnicas de investigação, mas também faz com que a própria técnica de incriminação seja alterada, com a antecipação da intervenção penal. Como afirma Hassemer[336],

> No moderno direito penal pode-se constatar com frequência que as diferenciações dogmáticas entre imputação objetiva e subjetiva, que oferece critérios racionais e controláveis, ficam esmaecidas. Distinções como as de autoria e participação, tentativa de consumação, dolo e culpa, características do direito penal tradicional, se transformaram no moderno direito penal em termos como "traficar" ou "empreender", que deslocam os conceitos clássicos para um secundário, quando não os anula por completo", ampliando-se, em consequência disso, o arbítrio judicial, dificilmente controlável e pouco verificável com critérios dogmáticos.
> [...]
> Também o mandato de certeza, [...] é desprezado pelo moderno direito penal. Desde que uma criminalização o mais precisa possível, tal como exige o direito penal do Estado de direito, constitui um obstáculo para uma criminalização mais ampla e superficial. Porém é exatamente isso que o moderno direito penal pretende: ser suficientemente flexível e onicompreensivo para responder adequadamente às perturbações cambiantes contínuas. E o mandado de certeza é, por certo, um obstáculo para um direito flexível e adaptável aos problemas cambiantes que podem se apresentar no futuro[337]

Essas necessidades político-criminais são todas ligadas à precaução, isto é, à tentativa de se evitar o incremento de atividades potencialmente perigosas (dado que sequer os perigos futuros são certos), o que gera um direito penal substancialmente diverso daquele defendido pelo garantismo, voltado essencialmente à tutela de bens personalistas e do patrimônio.

---

336 HASSEMER, Winfried. **Persona, mundo y responsabilidad. Bases para una teoria de la imputación em derecho penal.** Editorial Temis: Santa Fe de Bogotá – Colômbia, 1999. p. 28

337 Tradução Nossa. No original: " En el moderno derecho penal se puede constatar frecuentemente que las diferenciaciones dogmáticas entre imputación objetiva y subjetiva, que ofrecen criterios racionales y controlables, quedan difurninadas. Distinciones como las de autoría y participación, tentativa y consumación, dolo e imprudencia, características del derecho penal tradicional, se han transformado en el moderno derecho penal en términos tales como "traficar" o "emprender", que desplazan los conceptos clásicos a un lugar secundario, cuando no los anulan por completo", ampliándose, a consecuencia de ello, el arbitrio judicial, difícilmente controlable y poco verificable con criterios dogmáticos.

[...] También el mandato de certeza, [...] es conculcado por el moderno derecho penal. Desde luego que una criminalización lo más precisa posible, tal como exige el derecho penal del Estado de derecho, constituye un obstáculo para una criminalización más amplia y superficial. Pero eso es precisamente lo que el moderno derecho penal pretende: ser lo suficientemente flexible y omnicomprensivo como para responder adecuadamente a las continuamente cambiantes perturbaciones. Y el mandato de certeza es, por supuesto, un obstáculo para un derecho flexible y adaptable a los cambiantes problemas que puedan presentarse en el futuro."

Em uma feliz síntese, Luis Gracia Martín[338] enumera as críticas à expansão "modernizadora" do direito penal, feitas por autores que adotam um discurso de resistência. Segundo ele, os autores comprometidos com o modelo garantista afirmam que a expansão do direito penal, além de representar uma massiva ruptura com as garantias penais de caráter liberal, apresenta três características que marcam sua distinção em relação ao modelo clássico:

1) Os objetos protegidos pelo "novo" direito penal, em especial o econômico e o do meio ambiente, não seriam verdadeiros "bens jurídico-penais", na medida em que não podem ser reconduzidos à condição de interesses diretamente ligados ao indivíduo, de modo que configurariam apenas "funções", instituições ou objetivos, constituindo, "em síntese, apenas objetos fictícios de tutela, que servem como pretexto para uma ampliação das incriminações";

2) além de tutelar objetos inidôneos, o moderno direito penal também lançaria mão de uma forma de intervenção ilegítima, antecipando a consumação do crime para um momento anterior ao de produção das lesões, criminalizando não o dano, mas a causação de um risco, já que a técnica dos tipos de lesão (crimes que exigem um dano ao bem jurídico, como o homicídio) ou de perigo concreto (quando o perigo deve ser demonstrado para a caracterização do crime, como no incêndio) vem sendo abandonada e, cada vez com mais frequência, é substituída pela técnica dos crimes de perigo abstrato, onde não se exige lesão de um bem jurídico ou a colocação deste bem em risco real e concreto, bem como onde o tipo descreve apenas uma conduta, sem exigir um resultado específico como elemento do injusto, característica que "atingiria magnitudes exponenciais no caso da proteção de substratos coletivos, já que suas gigantescas dimensões tornam praticamente impensável que a conduta individual e isolada de um sujeito determinado possa lesá-los ou expô-los a perigo";

3) o direito penal moderno assumiria um caráter apenas simbólico, em razão de sua perda de conexão com o bem jurídico, o que geraria, consequentemente, o abandono do princípio da lesividade, já que as incriminações feitas pelo legislador teriam como únicas finalidades produzir na sociedade e nos indivíduos a sensação de que, com a criminalização de novos comportamentos, o Estado está dando uma solução eficaz ao problema dos novos riscos ou, ainda, a incriminação teria um caráter meramente pedagógico (e, nesse sentido, também exclusivamente simbólico), voltada a criar na população a consciência da necessidade de respeitar determinados valores. Neste último sentido, trata-se de um direito penal que, ao invés de criminalizar condutas que atacam bens relevantes para a sociedade, se

338 **A modernização do direito penal como exigência da realização do postulado do estado de direito (social e democrático)**. Revista Brasileira de Ciências Criminais, vol. 88, p. 95

utiliza do aparato repressivo estatal para tornar relevante para a sociedade o respeito a determinados bens.

Em que pese não concordarmos com a conclusão desses autores quanto à ilegitimidade dessa nova forma de intervenção penal, o diagnóstico se apresenta como correto. No direito penal do risco, como afirma Pierpaolo Bottini[339], "o desvalor do resultado é substituído pelo desvalor da ação, o prejuízo concreto é substituído pela probabilidade de afetação de bens e interesses. Os tipos penais deixam de abrigar a lesão em sua redação e direcionam seus elementos ao perigo, ao risco". Nesse aspecto, o papel das novas tecnologias de informação e comunicação, em especial o aparato utilizado para a vigilância, é extremamente relevante na efetiva implementação desse modelo.

Com efeito, a partir do momento em que as dificuldades técnicas ou decorrentes da escassez de recursos para implementar a vigilância deixaram de representar um grande obstáculo à generalização da vigilância eletrônica, os limites externos à expansão do direito penal deixam de existir, por isso que a delimitação da atuação estatal em matéria de persecução penal, especialmente no que diz respeito aos métodos de coletas de prova, passaram a depender cada vez mais da construção de limites doutrinários e legais, fundados em uma dogmática orientada para a tutela das liberdades fundamentais. Sobre o tema, Fragoso e Rodrigues[340] chamam atenção para o fato de que, nas últimas décadas, ocorreu uma extraordinária expansão dos meios ocultos e sigilosos de investigação, que tradicionalmente admitem que os direitos fundamentais dos investigados sejam restringidos com fundamento na primazia do interesse público relacionado ao poder punitivo. Em um contexto de hiperconexão tecnológica e de facilidade de acesso a um conjunto massivo de dados, aliado a uma gigantesca capacidade de processamento de tais dados, a expansão do direito penal encontra solo fértil para se firmar na sociedade da informação.

Todo esse conjunto de fatores contribui para a institucionalização da utilização no âmbito do processo penal de métodos invasivos de investigação, inclusive por meio da aprovação de leis que passam a legitimar material e procedimentalmente a utilização de técnicas de vigilância que eram próprias da atividade de espionagem. Paralelo a isso, há uma inegável massificação da utilização de tais técnicas, que passam a ser utilizadas corriqueiramente, para a criminalidade comum, alcançando as esferas jurídicas de um número

339 BOTTINI, Pierpaolo Cruz. **Crimes de perigo abstrato.** 2ª. ed. São Paulo: RT, 2010.P. 88

340 FRAGOSO, NAthalie e RODRIGUES, Gabriel B. **Protodefesa à brasileira: contraditório e ampla defesa em investigações sigilosas.** Revista de Direito Público, Vol. 18, n. 100. out/dez 2021. pp. 581-605

inimaginável de indivíduos, independentemente de eles ostentarem ou não a condição de investigados.

Assim, tem-se que as expressões capitalismo de vigilância, sociedade da informação, sociedade do risco e capitalismo informacional configuram denominações para diferentes aspectos da sociedade contemporânea, que variam de acordo com o enfoque e os objetivos da análise. Entretanto, quaisquer que sejam essas dimensões em análise, um dado inegável é que todo esse conjunto de fatores fornece material e substrato para a expansão do direito penal, que não só passa a incluir a tutela de bens jurídicos diversos daqueles individuais, mas também passa a ser regido por uma espécie de abordagem precaucionária, na qual a antecipação da consumação do crime e a relativização de formalidades e garantias costumam dar a tônica.

O modelo de intervenção penal dirigido ao controle do risco é marcado pelo incremento da criminalização de comportamentos mediante a proliferação de novos bens jurídicos coletivos, pelo predomínio de estruturas típicas de crimes de mera conduta, especialmente pela criação de tipos de perigo abstrato, com a precaução substituindo em grande medida a lesividade como fundamento da incriminação e pelo recurso a leis penais que necessitam ser complementadas por normas administrativas - as leis penais em branco, além de se verificar uma evidente antecipação do momento da intervenção penal, criminalizando-se condutas que caracterizam atos meramente preparatórios. Por outro lado, ante a natureza difusa dos riscos e a enorme dificuldade de se individualizar com clareza a responsabilidade pelos eventuais danos, as garantias penais e processuais são flexibilizadas, facilitando a superação de dificuldades na imputação. No dizer de Díez Ripollés[341], no direito penal do risco,

> Se admitem certas perdas no princípio de segurança jurídica derivadas da menor precisão na descrição dos comportamentos típicos e do uso frequente da técnica das leis penais em branco; se faz uma interpretação generosa da lesividade real ou potencial de certos comportamentos, como na punição de determinadas posses ou no castigo de apologias; se considera razoável uma certa flexibilidade dos requisitos da causalidade ou da culpabilidade; se aproximam, até chegar às vezes a neutralizar-se, as diferenças entre autoria e participação, entre tentativa e consumação; se revaloriza o princípio de disponibilidade do processo, mediante a acreditação do princípio de oportunidade do processo e da negociação entre as partes; a agilidade e a celeridade do procedimento são objetivos suficientemente importantes para

341 DIÉZ RIPOLLÉS. José luis. **De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado.** RECPC 07-01 (2005) - http://criminet.ugr.es/recpc/07/recpc07-01.pdf. P. 05

> conduzir a uma significativa redução das possibilidades de defesa do acusado.[342]

Diante das condições atuais, uma vez que a tecnologia de vigilância em massa já se tornou extremamente acessível e deixou de ser um fator limitante, cresce ainda mais a importância da correta definição de limites éticos e legais para a proteção dos direitos fundamentais do indivíduo ante a atividade de persecução estatal, o que aumenta a importância da discussão dogmática acerca dos limites ao direito penal;

É imperioso, portanto, o enfrentamento da questão de se saber até que ponto o direito penal está apto a responder às necessidades da sociedade de risco, da sociedade de informação ou do capitalismo informacional, ante a conformação que lhe deram os ideais iluministas de controle do Estado pela legalidade estrita e pelo princípio da intervenção mínima.

A dizer, em um mundo cada vez mais marcado pela dependência de processos tecnológicos relacionados à obtenção de dados e informações dos indivíduos, onde o poder decorrente do acesso aos dados é distribuído e exercido de forma extremamente desigual, ante a falta de capacidade dos cidadãos de proteger sua privacidade diante das empresas de tecnologia e, consequentemente, diante da potencial atuação das autoridades públicas encarregadas da persecução penal com base na utilização secundária de tais dados, é preciso saber quais os limites de proteção de dados devem ser assegurados aos cidadãos. Na verdade, a resposta a essa pergunta diz respeito à própria adequação do Estado de Direito e de suas instituições a esse novo tempo de mudanças rápidas e de riscos generalizados, passa necessariamente pela compreensão dos limites epistemológicos à produção da prova em matéria penal.

4.3 BUSCA DA VERDADE E LIMITES EPISTEMOLÓGICOS À PROVA PENAL

O exercício do poder punitivo do Estado deve ser dirigido à proteção de bens jurídicos. Trata-se de um poder-dever instrumental, por isso que, em última análise, o direito

---

342 "Se admiten ciertas pérdidas en el principio de seguridad jurídica derivadas de la menor precisión en la descripción de los comportamentos típicos y del uso frecuente de la técnica de las leyes penales en blanco; se hace una interpretación generosa de la lesividad real o potencial de ciertos comportamientos, como en la punición de determinadas tenencias o en el castigo de apologías; se considera razonable una cierta flexibilización de los requisitos de la causalidad o de la culpabilidad; se aproximan, hasta llegar a veces a neutralizarse, las diferencias entre autoría y participación, entre tentativa y consumación; se revaloriza el principio de disponibilidad del proceso, mediante la acreditación del principio de oportunidade procesal y de las conformidades entre las partes; la agilidad y celeridad del procedimento son objetivos lo suficientemente importantes como para conducir a una significativa reducción de las posibilidades de defensa del acusado." (tradução nossa).

penal deve ser compreendido como um meio de tutela de direitos fundamentais. Nessa perspectiva, o direito penal deixa de ser visto como mero instrumento de dominação e controle, como simples expressão do monopólio estatal da violência, e passa a ser entendido como a mais poderosa arma de que dispõe o Estado para a tutela de direitos fundamentais.

Por isso, o poder punitivo somente é legitimamente exercido por meio do devido processo penal, instrumento legal que permite verificar se uma imputação é verdadeira e possibilita a aplicação das sanções previstas, caso se conclua que realmente o réu praticou a conduta típica, antijurídica e culpável que lhe é atribuída. A existência de um processo em que sejam asseguradas a seus partícipes as garantias processuais fundamentais é essencial para que o exercício do poder punitivo do Estado seja legítimo.

Não basta a mera obediência formal ao procedimento para que o resultado do processo possa ser qualificado de justo. De fato, uma concepção de justiça e legitimidade do processo que se encerre na correção do procedimento seria claramente insuficiente. Na realidade, para cumprir corretamente sua função de instrumento de efetiva tutela de direitos fundamentais, o direito penal e o direito processual penal precisam agregar também um adequado exercício da atividade epistêmica, que possibilite a reconstituição correta dos fatos em julgamento, e uma correta atividade hermenêutica, que garanta a aplicação adequada das normas aos fatos apurados, sendo que tanto a atividade epistêmica quanto a hermenêutica devem ser exercidas seguindo o devido processo legal, para que se possa chegar a uma decisão justa.

Assim, conforme alerta Taruffo[343], a justiça de uma decisão judicial não se exaure no procedimento adotado, mas necessita da subsistência de três condições específicas, que precisam ser cumpridas concomitantemente: a) que a decisão seja resultado de um *processo justo*, no qual os fatos são discutidos e o direito é aplicado através de um procedimento que possibilite que as partes exerçam amplamente sua defesa e o contraditório, na discussão dos fatos e do direito; b) que a norma aplicada como critério de validade ao caso tenha sido resultado de uma correta atividade hermenêutica; c) que a aplicação da norma se funde numa adequada reconstrução histórica dos fatos imputados ao réu.

A conjugação desses três elementos como requisitos de uma decisão justa realça a ligação entre a reconstituição dos fatos e a legitimidade da persecução penal. Nessa perspectiva, tem-se que há uma inegável vinculação entre o direito penal e a busca pela

[343] TARUFFO, Michele. **Uma simples verdade. O juiz e a reconstrução dos fatos.** São Paulo: Marcial Pons, 2012. p. 142.

"verdade" ou pela certeza acerca dos fatos que são objeto do processo, dado que, como afirma Taruffo[344],

> A apuração da verdade dos fatos correspondentes ao chamado suporte fático regulado pela norma é uma *condição necessária* para a correta aplicação da norma no caso concreto: a veracidade da apuração dos fatos é um requisito essencial da legalidade da decisão. Por conseguinte, não só a verdade dos fatos não é irrelevante, como também (e ao contrário disso) condiciona e determina a correção jurídica da solução da controvérsia.

Evidentemente que não estamos aqui nos referido a uma suposta busca pela "verdade real", como se pudesse existir algo como uma "verdade absoluta" que não fosse mediada pela linguagem e pela consciência[345], mas tão somente reforçamos a ideia de que a busca pela verdade dos fatos, como ideal a orientar a atividade de instrução praticada no processo, é requisito essencial para o exercício do poder punitivo no estado democrático de direito.

De fato, a proteção de bens jurídicos como *ultima ratio* é a tarefa essencial do direito penal material, e, para fazer isso são tipificadas condutas que lesionem ou coloquem em riscos os bens tutelados. A função específica do tipo penal, do ponto de vista de sua funcionalização político-criminal, é permitir que os destinatários da norma saibam quais são as condutas proibidas pela norma e, assim, possam dirigir suas ações para evitar a prática de tais fatos típicos. Por outro lado, a imposição da sanção que terá o efeito retributivo e preventivo (geral e específico) pressupõe a existência de provas suficientes para demonstrar, além de uma dúvida razoável, que o fato típico realmente aconteceu.

O direito processual penal, portanto, deve ser estruturado para levar ao esclarecimento da verdade. Como afirma Schünemann[346], "a aptidão para a descoberta da verdade ainda constitui o ponto arquimédico para todo e qualquer instituto de processo penal" e os limites da cognição humana não são suficientes para infirmar o valor da busca pela verdade na persecução penal. Aliás, vale ressaltar que as teorias da verdade como correspondência, que

---

[344] TARUFFO, Michele. OP. Cit. p. 140

[345] A questão da verdade é dos mais antigos e persistentes problemas filosóficos, sendo de grande interesse para os juristas, especialmente após o giro linguístico e da obra de filósofos como Heidegger, Gadamer e Wittigenstein. Obviamente, entretanto, aqui não nos ocuparemos dessa questão aqui, nem mesmo da correlata questão epistêmica da busca pela verdade "processual" ou às teorias processuais que decorrem da concepção adotada. Sobre esse tema, consultar a obra de Michele Taruffo, que dedicou quase toda sua produção acadêmica ao trinômio fundamentação - prova - verdade, valendo consultar especialmente **a prova** e **Uma simples verdade**, ambas publicadas no Brasil pela Marcial Pons e **La prueba de los hechos,** publicado na Espanha pela Editorial Trotta.

[346] SCHÜNEMANN, Bernd. **Estudos de direito penal, direito processual penal e filosofia do direito.** São Paulo: Marcial Pons, 2013, p. 245.

sustentam que "a verdade" é a correspondência entre ideias ou conceitos e objetos[347], equivalem à construção social da realidade, algo que se concretiza especificamente no reino da linguagem, como fenômeno essencialmente social e, por isso, se adequa perfeitamente ao processo penal, também fenômeno essencialmente social e comunicativo.

Nesse aspecto, tem-se que a reconstrução dos fatos imputados ao réu é provavelmente a atividade mais relevante desempenhada no processo, uma vez que processos penais se destinam precipuamente a possibilitar que, dentro dos limites legais, se possa apreciar a veracidade de uma imputação penal, isto é, verificar a ocorrência de fato concreto subsumível a uma norma penal e sua autoria. Comprovado que o réu praticou o fato típico, antijurídico e culpável que lhe é imputado, a ele serão aplicadas as sanções legalmente previstas. Do contrário, seja pela demonstração de que o fato não ocorreu ou que o acusado não foi seu autor, ou simplesmente porque as provas produzidas não permitem concluir pela materialidade e autoria acima de uma dúvida razoável, o resultado deverá ser a absolvição, com a manutenção do estado de inocência do acusado.

Por isso que um processo penal é sempre uma "máquina retrospectiva", que tem como objetivo primordial a reconstituição de um fato passado com vista a determinar se um fato ocorreu e quem foi seu autor, a partir de um procedimento em que as partes formulam hipóteses e no qual cabe ao juiz, com base em um conhecimento empírico, acolher a mais provável, com estrita observância de determinadas normas[348].

Não cabe aqui aprofundar as ricas discussões filosóficas acerca da ideia de que a verdade é inalcançável (posto que somente conseguimos obter versões da verdade) ou seu reflexo no campo processual, materializada na ideia de que, por meio do processo judicial, não se pode pretender chegar à chamada "verdade real", mas tão somente à uma verdade formal, construída a partir do que foi colhido na instrução processual. Entretanto, quaisquer que sejam as abordagens adotadas, importa ressaltar que a busca da verdade sobre os fatos discutidos nos autos sempre é um imperativo de justiça. Com efeito, como afirma Leonardo Greco[349],

---

[347] CF COLARES DO NASCIMENTO, Matheus. **Teorias da verdade como correspondência.** PÓLEMOS – Revista de Estudantes de Filosofia da Universidade de Brasília, v. 9, n. 18, p. 293–314, 2020. Disponível em: https://periodicos.unb.br/index.php/polemos/article/view/29581.

[348] Cf. LOPES JR, Aury. Direito **Processual Penal e sua conformação constitucional**. Vol I . p. 523

[349] GRECO, Leonardo. O conceito de prova. Revista da Faculdade de Direito de Campos, Ano IV, Nº 4 e Ano V, Nº 5 - 2003-2004, pp. 233-234

> Em todos os tempos, a idéia de Justiça como objeto do Direito sempre esteve axiologicamente ancorada no pressuposto da verdade, ou seja, na incidência das normas jurídicas sobre a realidade da vida tal como ela é. Os indivíduos somente se sentem eticamente motivados a conviver sob o império da lei, quando sabem que a justiça vai dar a cada um o que é seu, em conformidade com a verdade. É claro que na História da Humanidade, em muitas épocas o conceito de verdade, como *adequatio intellectus ad rem*, foi questionado pelos filósofos, ou foi considerado inacessível ou foi sobrepujado pelo Estado autoritário ou pelo positivismo, mas sempre, na teoria das provas, a verdade ou a certeza dos fatos ressurge como uma função importante. Jeremias Bentham, escrevendo no início do século XIX, após o impacto do racionalismo cartesiano e do idealismo kantiano, ironiza os filósofos, que duvidam da própria realidade do mundo físico, dizendo que os que os seguirem piamente correrão o risco de não se afastarem de um carro que avança ou de um rio à sua frente, e, assim, "destrozaréis o ahogaréis um gran filósofo."

Tem-se, pois, que mesmo a despeito de se reconhecer as dificuldades imanentes à busca pela verdade no processo, o Direito não pode abdicar desta finalidade, que deve sempre figurar como horizonte de sentido a guiar toda a atuação dos operadores do direito. Com efeito, render-se ao relativismo exagerado, tão ao gosto de algumas teorias procedimentalistas que enxergam no processo unicamente um meio de solução de conflitos, sem compromisso com a verdade dos fatos ou com a justiça da decisão, implicaria em negar ao direito seu caráter de ciência instrumental dotado de uma pretensão de correção. Nesse sentido, vale lembrar a magistral lição de Ferrajoli[350], que adverte que se uma justiça penal "inteiramente 'como verdade' constitui uma utopia, uma justiça penal inteiramente 'sem verdade' equivale a um sistema de arbítrio". Por isso é que o exercício legítimo do poder em matéria penal pressupõe sua complementação pelas noções de justiça e verdade.

Cabe notar, ainda, que a disciplina concreta dos institutos processuais, mais do que decorrência de simples escolhas técnicas, é fruto de uma opção politicamente orientada. A normatização dos elementos e requisitos de um ato processual, dos sujeitos legitimados a requerê-lo, da forma como deve ser praticado, bem como das provas admissíveis ou não para a reconstrução de um fato, são também, escolhas de valor[351].

A atividade probatória exercida no âmbito de um processo penal que se pretenda democrático, pois, deve conciliar a pretensão de realização da justiça, fundada na maior

---

[350] FERRAJOLI, Luigi. **Direito e razão. Teoria do garantismo penal.** p. 19

[351] CF. BADARÓ, Gustavo. **Editorial dossiê "Prova penal: fundamentos epistemológicos e jurídicos".** Revista Brasileira de Direito Processual Penal. Vol. 4, n. 1, 2018. disponível em https://revista.ibraspp.com.br/RBDPP/article/view/138/117

aproximação possível da verdade histórica, com o respeito aos direitos fundamentais do investigado/acusado. Como ensina Muñoz Conde[352],

> [...] o Processo Penal de um Estado de Direito deve não somente manter um equilíbrio entre a busca da verdade e a dignidade dos acusados, mas deve entender a verdade mesma não como como uma verdade absoluta, mas sim como o dever de fundamentar uma condenação somente sobre aquilo que indubitável e intersubjetivamente pode ser dado como provado. O resto é puro facismo e volta aos tempos da inquisição, dos quais se supõe já havermos felizmente saído[353].

É de se notar, entretanto, que a afirmação de que a busca da verdade deve ser um guia a orientar o processo penal não implica que se possa admitir tudo e qualquer coisa em nome da busca da verdade. Há limites quanto à atividade de reconstituição dos fatos, que são verdadeiros marcos civilizatórios e decorrem do respeito à dignidade humana. Com efeito, em nosso regime jurídico-constitucional toda atividade estatal deve necessariamente ser realizada atendendo aos princípios e às regras constitucionais que conferem direitos fundamentais aos indivíduos e que, por óbvio, não podem ser desconsiderados em nome de razões eficientistas da pretensa busca pela "verdade real". Não se pode desconhecer o fato de que, na precisa lição de Ferrajoli[354],

> É evidente que esta pretendida "verdade substancial", ao ser perseguida fora das regras e controles, e sobretudo, de uma exata predeterminação empírica das hipóteses de indagação, se degenera em um juízo de valor, amplamente arbitrário de fato, assim como a cognição ética sobre aquilo em que se baseia o substantivismo penal resulta inevitavelmente solidário com uma concepção autoritária e irracionalista do Processo penal.

A Constituição Federal traz limitações expressas à atividade persecutória estatal quando, *v.g*, elege à condição de direitos fundamentais a intimidade (art. 5º, X), a inviolabilidade do domicílio (inciso XI), a inviolabilidade do sigilo da correspondência e das

---

[352] MUNÕZ CONDE, Francisco Búsqueda de la **Verdad en el Proceso Penal**, Buenos Aires: Depalma: 2000, p. 107.

[353] Tradução nossa. No original: "el proceso penal de un Estado de Derecho no solamente debe lograr el equilibrio entre la búsqueda de la verdad y la dignidad de los acusados, sino que debe entender la verdad misma no como una verdad absoluta, sino como el deber de apoyar una condena sólo sobre aquello que indubitada e intersubjetivamente puede darse como probado. Lo demás es puro fascismo y la vuelta a los tiempos de la Inquisición, de los que se supone hemos ya felizmente salido" tradução livre".

[354] FERRAJOLI, Luigi. **Direito e razão. Teoria do garantismo penal.** p. 45

telecomunicações (inciso XII) e inadmissibilidade das provas obtidas por meios ilícitos (inciso LVI). Mais recentemente, a Constituição inclusive passou a prever no rol de direitos fundamentais a "proteção de dados, inclusive nos meios digitais" (art. 5º, LXXIX), como direito autônomo. Da mesma forma, o pacto de São José da Costa Rica, que integra o ordenamento jurídico interno, prevê em seu art. 11º, que

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade;

2. ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação;

3. toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.".

Tais marcos, portanto, representam um limite à busca dos órgãos estatais por elementos que possibilitem a persecução penal, configurando verdadeiros limites éticos à atividade probatória. Como afirma Maria Thereza Assis Moura[355]

> No que concerne aos limites éticos, repousam eles na legitimidade moral da formação da prova, que respeite a privacidade ou a intimidade, enfim, a plena liberdade do homem e, sua vida íntima, daí porque o processo deve se desenvolver dentro de uma escrupulosa regra moral, que orienta a atividade do juiz e das partes em prol do valor essencial da dignidade da pessoa humana.

Assim, se o que se busca é a concretização de um processo penal democrático, compatível com os ditames do Estado de Direito, em que toda atividade estatal seja desenvolvida dentro de um conteúdo ético que lhe conceda legitimidade, é preciso não se relativizar os limites da ação probatória dos órgãos da persecução penal, estabelecendo-se, a partir de uma valoração de bens constitucionalmente protegidos como a dignidade da pessoa humana, a privacidade e a intimidade, o que é a prova vedada e quais são os efeitos da declaração da ilicitude sobre o processo.

As provas vedadas ou ilegais configuram gênero do qual as provas ilegítimas e ilícitas são espécies. As provas ilegítimas são aquelas cuja produção implica na violação de uma regra de direito processual (ex. juntada de documento fora de prazo, inquirição de testemunha proibida de depor etc). As provas ilícitas, por seu turno, são as produzidas com violação dos

[355] MOURA, Maria Thereza de Assis. **A ilicitude na obtenção da prova e sua aferição**. Palestra proferida no I Seminário no Estado de Minas Gerais – V Seminário Regional do IBCCRIM- Uberlândia, no dia 5 de dezembro de 1997. Disponível em www.ambitojurídico.com.br

direitos fundamentais do indivíduo, cuja produção implique na agressão a um direito material ou constitucional, sendo a ilicitude sempre relacionada a um dado que está fora do processo (ex. gravação telefônica clandestina, obtenção de depoimento mediante coação). A distinção é importante porque as provas ilícitas não podem em momento algum ser convalidadas ou repetidas, ao passo que as ilegítimas podem, em tese, ser repetidas, uma vez afastada a violação processual que ensejou sua ilegitimidade. Neste ponto, releva notar que a Lei 11.690/2008, buscando dar concreção à norma constitucional que determina a inadmissibilidade das provas obtidas por meios ilícitos, alterou o art. 157 do CPP, que passou a ter a seguinte redação:

> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (Redação dada pela Lei nº 11.690, de 2008)
>
> § 1o. São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008).
>
> § 2o. Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. (Incluído pela Lei nº 11.690, de 2008)
>
> § 3o. Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente. (Incluído pela Lei nº 11.690, de 2008)

Verifica-se, assim, que a distinção entre provas ilícitas e ilegítimas não foi acolhida pelo legislador, que tratou como "ilícitas" ambas as modalidades, porém essa distinção remanesce útil como critério para balizar uma eventual decisão acerca da possibilidade da repetição da prova.

Outra classificação das limitações à produção de provas é a que diz respeito aos fundamentos da exclusão, separando limitações referentes à própria aptidão da prova para reconstituir o fato daquelas fundadas em fatos extraprocessuais, mais relacionados a critérios políticos. Esta é uma distinção muito utilizada nos países do *Common Law*, onde as restrições internas (*intrinsic policy*) servem precipuamente à finalidade de evitar que uma prova falha (do ponto de vista de sua confiabilidade e aptidão para efetivamente demonstrar a ocorrência

ou não de um fato) possa "contaminar" os jurados[356]. São exemplos de restrições internas a exigência prevista no art. 158 do CPP, de que seja realizado exame de corpo de delito nas infrações que deixam vestígio, vedando que a confissão do acusado possa suprir tal modalidade de prova. Também se enquadram nesta categoria de restrições os testemunhos prestados por pessoas que não prestam compromisso de dizer a verdade (art. 208 do CPP), a prova relativa ao estado das pessoas, que deve seguir as regras da lei civil (parágrafo único do art. 155 do CPP) e as provas impertinentes, desnecessárias ou meramente protelatórias.

Por outro lado, as restrições decorrentes de fatores extra-processuais refletem o fato de que a atuação estatal de persecução penal deve ser realizada sempre dentro dos limites moralmente aceitáveis e politicamente legítimos. Por isso que é de todo inadmissível a atividade probatória que, mesmo sendo apta a demonstrar a veracidade dos fatos em julgamento, tenha sido obtida por meios ilícitos. Trata-se de reconhecer que valores estranhos ao processo penal devem ser por ele tutelados também, ainda que essa tutela implique no sacrifício da busca pela verdade.

Com efeito, no campo do processo penal, os fins nunca podem justificar os meios e valores como a dignidade da pessoa humana, a proteção à intimidade e a privacidade devem ser levados em conta para a definição do âmbito legítimo da atividade probatória. Por isso que, por exemplo, uma confissão obtida mediante tortura, uma interceptação telefônica realizada sem autorização judicial ou uma prova obtida mediante invasão de domicílio são nulas e não só devem ser desentranhadas dos autos, mas também contaminam todas as provas delas decorrentes. Na *Common Law* essas regras de exclusão (denominadas de *exclusionary rules of extrinsic policy*) são constituídas pelos *privileges,* que protegem a esfera jurídica dos cidadãos contra a atuação estatal. São normas fundadas na necessidade de proteção de direitos considerados essenciais para o indivíduo. Para Gomes Filho[357], a restrição às provas fundada em fatores extrínsecos ao processo

> Cuida-se, em síntese, de preservar a esfera individual contra intromissões que, embora ditadas pelo interesse de eficiência do processo, poderiam ter um custo desproporcional na ótica de uma organização social secularmente assentada na primazia do indivíduo.

[356] GOMES FILHO, Antonio M. **Direito à prova no processo penal**. São Paulo: RT, 1997. p. 96 e ss..

[357] GOMES FILHO, Antonio M. **Direito à prova no processo penal**. São Paulo: RT, 1997. p. 99.

4.4. PRIVACIDADE COMO LIMITE EXTRÍNSECO À PRODUÇÃO DE PROVA

A proteção a valores extra processuais, criando limites à atuação probatória em matéria penal, reflete o fato de que o direito penal é um saber científico teleológico, que segue uma racionalidade instrumental que deve se caracterizar pela busca de integração da dogmática jurídico-penal às razões de política criminal. Por isso, a dogmática jurídico-penal deve estar sempre atenta à necessidade de cumprir finalidades valorativas, de cunho preventivo-repressiva, de modo a possibilitar que, como afirma Roxin[358], funcione o direito penal como "a forma através da qual as finalidades político-criminais podem ser transferidas para o modo da vigência jurídica".

A tutela constitucional da privacidade, em todas as suas dimensões, não é matéria de cunho apenas civilístico ou administrativo, mas gera profundos efeitos também sobre a persecução penal que vão muito além da mera discussão acerca da publicidade do processo e da eventual exposição do investigado/réu/condenado à opinião pública. Na verdade, a privacidade no campo penal é mais ampla, posto que inclui, entre outros aspectos, também as discussões acerca dos limites à sujeição do investigado à atividade probatória, por isso que a privacidade tem também uma dimensão coletiva que, no campo penal, constitui uma esfera de proteção ao indivíduo, instituindo limites para a intervenção das agências estatais encarregadas da investigação de crimes e de buscar judicialmente a condenação.

Ressalte-se que essa afirmação não quer significar que, para efeitos penais, apenas a dimensão individual da privacidade deva ser considerada. Obviamente, tais aspectos são de absoluta importância como expressões da dignidade humana, seja no que diz respeito à proteção ao nome/imagem do investigado, seja (especialmente) em sua vertente de limitação de acesso a aspectos da intimidade (e aqui entram todas as limitações e restrições à produção de provas invasivas). Porém, também no campo penal deve-se ter em conta que a privacidade é um conceito multifacetado e que tanto tem dimensões individuais como dimensões coletivas de modo que, ao se pensar na tutela da privacidade no campo penal, não só a proteção à esfera de intimidade do indivíduo cumpre um importante papel coletivo, demarcando os limites da atuação estatal, mas também as outras dimensões da privacidade são relevantes.

Veja-se que a concepção da privacidade como controle é também um importante elemento para se pensar, por exemplo, no cabimento da autodeterminação informativa em matéria penal, o que, de resto, foi expressamente previsto no anteprojeto da lei de proteção de

[358] ROXIN, Claus. **Política criminal e sistema jurídico-penal.** Rio de Janeiro: Renovar, 2000, p. 82

dados elaborado pela comissão de juristas coordenados pela Professora Laura Schertel e encaminhado ao Congresso Nacional em 5 de novembro de 2020. Em sua exposição de motivos, os autores do anteprojeto afirmam que a proposta legislativa pretende oferecer balizas e parâmetros que garantam um equilíbrio entre a proteção do titular contra a violação de seus direitos individuais e o tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal.

O anteprojeto prevê em seu artigo 2º, II, a autodeterminação informativa como um dos fundamentos para a disciplina da proteção de dados pessoais para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. Tendo em conta que a autodeterminação informativa consiste, em última análise, no controle pelo titular acerca do trânsito de seus dados, configurando uma extensão da liberdade do indivíduo, tem-se que a forma de aplicação de tal direito autônomo em sede de persecução penal requer, no mínimo, algumas adaptações em relação à configuração cível da autodeterminação informativa.

Isso porque a obtenção de informações e dados pessoais necessários para a instrução criminal não pode contar com a participação voluntária do investigado, mas deve ser feita pelos órgãos encarregados da investigação e da persecução de forma independentemente da participação ou mesmo da concordância do investigado, forte no princípio do *nemo tenetur se detegere*. Por isso, ante o privilégio contra a autoincriminação, tem-se que a compreensão da autonomia informacional em matéria penal deve levar em conta as expectativas razoáveis de proteção de que fala Nissenbaum, de modo a possibilitar um efetivo equilíbrio entre a privacidade (contextual) e a segurança pública.

Nesse sentido, a Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro (Enccla) apresentou em dezembro de 2021 uma nota técnica[359] em que afirma:

> Relativamente ao direito de autodeterminação informativa, pilar do direito à proteção de dados pessoais, este é visto como fundamento necessário, porém **cuja avaliação deve ser realizada em conjunto com outros fundamentos** que desaconselhem a uma leitura absoluta de referido direito. Nesse sentido, propõe-se a inclusão de

[359] ESTRATÉGIA NACIONAL DE COMBATE AOS CRIMES DE CORRUPÇÃO E LAVAGEM DE DINHEIRO. **Ação 04/2021.** Nota Técnica contendo a avaliação, propostas de alterações, contrastando o texto do anteprojeto com Convenções, recomendações e melhores práticas internacionais, em relação ao Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal – LGPD-Penal. Disponível em http://enccla.camara.leg.br/acoes/acoes-de-2021

> fundamentos adicionais, dentre os já existentes na norma, que robusteçam os meios de ponderação entre os direitos tutelados:
>
> VIII - dever estatal de eficiência, por meio da previsão de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais, sem incorrer em preconceitos de qualquer natureza;
>
> IX - a proteção de direitos individuais e difusos, por meio da aplicação de sanções civis ou penais proporcionais à gravidade das violações;
>
> X - a observância do princípio da proibição da proteção deficiente de bens jurídicos de extração constitucional;
>
> XI – respeito ao direito à segurança.

A proposta de se adequar o direito de autonomia informacional às finalidades preventivas e repressivas próprias da seara criminal, independentemente de qualquer avaliação acerca do mérito da discussão, que é essencialmente política, ressalta a importância da compreensão da privacidade em suas diversas dimensões, especialmente a partir da concepção contextual de Nissenbaum.

A abordagem da privacidade de forma contextual, ligada às normas e expectativas sociais, também se mostra relevante na compreensão do papel que a privacidade exerce no curso de toda a atividade persecutória do Estado. Cabe lembrar que o processo penal tem um desenvolvimento escalonado, onde a cada fase há uma maior interferência sobre a esfera personalíssima de proteção ao indivíduo e, exatamente por isso, há exigências maiores a serem cumpridas pelos agentes estatais.

Assim é que, para a instauração de uma investigação formal, é suficiente a existência de uma informação qualquer que indique a ocorrência de um crime (desde que dotada de alguma credibilidade, como não ser proveniente de fonte anônima ou trazer algum indício material); para o indiciamento, é necessária a existência de um feixe convergente de indícios que permitam a autoridade policial, após análise técnico-jurídica do fato “indicar a autoria, materialidade e suas circunstâncias”, nos termos do § 6º do art. 2º da Lei 12.830/2013; para o recebimento da denúncia, são necessários indícios suficientes de autoria e prova da materialidade da ocorrência do crime, e, para uma condenação, é necessário que existam

provas suficientes para que se conclua, acima de uma dúvida razoável, que o crime efetivamente ocorreu e de que o réu foi o autor.

Da mesma forma, a imposição de medidas cautelares de natureza criminal também segue um escalonamento em seus requisitos, que variam de acordo com o grau de interferência na esfera de liberdade. Por isso que, para uma busca e apreensão de documento, por exemplo, são suficientes, nos termos do disposto no art. 240 e ss. do CPP, o *periculum in mora*, consubstanciado no risco de desaparecimento ou ocultação do documento que interessa à prova de uma infração penal, e o *fumus boni juris*, previsto no art. 240, §1°, do CPP, sob o conceito de "fundadas razões" e que consiste em: (a) um juízo de probabilidade quanto ao encontro do documento no local a ser revistado; (b) probabilidade de que os documentos procurados efetivamente tenham relação e relevância para a investigação de um fato criminoso; e, (c) indícios da existência do crime que se investiga. A noção de fundadas razões, necessárias à autorização da busca domiciliar, implica um juízo de ponderação previamente realizado pelo legislador penal que considerou o atendimento a esses requisitos suficiente para a decretação de uma medida cautelar invasiva da intimidade.

Por outro lado, deixando evidente a alteração dos requisitos como reflexo do juízo de proporcionalidade para uma intervenção mais gravosa, verifica-se que a decretação de uma medida mais restritiva de direitos fundamentais do investigado tem requisitos substancialmente mais rigorosos. Veja-se a prisão temporária, por exemplo. Nos termos da Lei 7.960/1989, essa medida somente é cabível quando imprescindível para as investigações do inquérito policial (art. 1º, inc. I), quando o indicado não tiver residência fixa ou não fornecer elementos necessários ao esclarecimento de sua identidade (art. 1º, inc. II), devendo haver "fundadas razões, de acordo com qualquer prova admitida na legislação penal, de autoria ou participação do indiciado" no rol de crimes previstos no inciso III.

Trata-se de requisitos significativamente mais estritos do que aqueles previstos para a busca e apreensão, refletindo a natural preocupação com a maior gravidade da intervenção sobre a esfera de intimidade do investigado, o que se tornou ainda mais evidente a partir da recente decisão do STF nas ADIs 4109 e 3360, na qual o Plenário determinou interpretação conforme à Lei 7.960/1989 para deixar claro que a prisão temporária somente é admissível quando, cumulativamente:

1) for imprescindível para as investigações do inquérito policial (art. 1º, I, Lei 7.960/1989) (*periculum libertatis*), constatada **a partir de elementos concretos, e não meras conjecturas, vedada a sua utilização como prisão para averiguações,** em violação ao

direito à não autoincriminação, ou quando fundada no mero fato de o representado não possuir residência fixa (inciso II);

2) houver fundadas razões de autoria ou participação do indiciado nos crimes previstos no art. 1º, III, Lei 7.960/1989 (*fumus comissi delicti*), **vedada a analogia ou a interpretação extensiva** do rol previsto no dispositivo;

3) for justificada em **fatos novos ou contemporâneos** que fundamentem a medida (art. 312, § 2º, CPP);

4) a medida for adequada à **gravidade concreta** do crime, às **circunstâncias do fato** e às **condições pessoais** do indiciado (art. 282, II, CPP); e,

5) **não for suficiente a imposição de medidas cautelares diversas**, previstas nos arts. 319 e 320 do CPP (art. 282, § 6º, CPP).

Essa diferenciação nos requisitos para a imposição de medidas que afetam a esfera de individualidade do investigado, denunciado ou réu, em um processo penal, reflete de modo muito evidente a existência de um juízo de proporcionalidade feito pelo legislador processual penal (que, em uma perspectiva mais ampla, atua regulando os limites de intervenção estatal sobre a esfera de liberdade e, por conseguinte, sobre a privacidade), mas que também vincula o julgador, quando da aplicação da lei processual aos casos concretos.

A privacidade, portanto, mesmo que de forma velada, é sempre um dos valores que estão em jogo quando se estabelecem os limites para atuação das agências estatais encarregadas pela persecução penal. O maior rigor nas medidas mais intrusivas reflete, na realidade, uma densificação da tutela da privacidade. Por isso, medidas menos gravosas podem ser determinadas à vista de elementos menos rigorosos ao passo que as medidas mais rigorosas têm requisitos mais rígidos. Ainda que esse fato não seja concretamente percebido, trata-se do reflexo da maior proteção conferida pelo ordenamento jurídico ao núcleo essencial do direito à privacidade.

Os requisitos são tanto mais rigorosos quanto mais invasiva for a medida. Há, por assim dizer, um equilíbrio entre a gravidade da intervenção penal e a tutela da privacidade que reflete, em última análise, um juízo de ponderação que deve ser feito, seja em abstrato, pelo legislador, na regulação das hipóteses de intervenção, seja em concreto, pelo juiz, ao apreciar o pedido feito pela polícia judiciária ou pelo Ministério Público.

Há que se reconhecer, portanto, que a privacidade atua como limite extrínseco à busca pela prova penal, por isso é que toda atividade probatória em matéria penal deve se dar de

forma controlada e regrada, já que a atividade investigatória sempre vulnera, em maior ou menor grau, algum aspecto da privacidade dos sujeitos investigados.

4.5 CONFLITOS ENTRE PRIVACIDADE DIGITAL E PROVA PENAL

A disciplina concreta da limitação à produção de provas em matéria criminal encerra sempre um juízo de ponderação entre a privacidade e a segurança pública. No mais das vezes, esse juízo, pelo menos no que concerne a seus aspectos mais gerais, é feito ainda no campo abstrato, pelo legislador, ao estabelecer requisitos e condições para a produção da prova. É o que ocorre no caso da interceptação telefônica, por exemplo, em que o legislador previu, no art. 2º da Lei 9.296/1996, que não será admitida a interceptação de comunicações telefônicas quando não houver indícios razoáveis da autoria ou participação em infração penal (inciso I); a prova puder ser feita por outros meios disponíveis (inciso II) ou quando o fato investigado constituir infração penal punida, no máximo, com pena de detenção. (inciso III).

A multiplicidade de situações e fatos da vida fazem com que não raro a regulamentação legislativa sobre as restrições e os limites de direitos fundamentais, em especial daqueles relacionados à produção de prova em feitos de natureza criminal, seja insuficiente para resolver as questões que se apresentam no cotidiano, sendo muito comum que surjam discussões acerca da validade da prova produzida tanto a partir dos limites abstratos quanto em face da produção concreta da prova.

Conflitos normativos são aquelas hipóteses em que, acerca de um mesmo fato ou conjunto de fatos, incide mais de uma norma determinando consequências diversas, pelo menos em parte. Neste ponto, vale salientar que, como forma de evitar as controvérsias acerca do conceito de norma, adotamos aqui o conceito de Kelsen, para quem normas seriam *atos de vont*ade emitidos pela autoridade competente, isto é, o legislador ou o administrador, nos casos das leis e regulamentos gerais, ou o juiz, no caso da sentença (valendo ressaltar que, na teoria kelseniana, a atividade judicial não é meramente declaratória, mas criadora de norma individual)[360].

Os conflitos entre regras são solucionados no campo da validade, pela revogação ou pelo estabelecimento de uma cláusula de exceção a partir de uma terceira norma, que regulamenta a solução do conflito. É o que ocorre, por exemplo, quando norma posterior

[360] KELSEN, Hans. **Teoria Geral das Normas.** Porto Alegre: Sergio Antonio Fabris editora. 1986, p. 1/2.

revoga as normas anteriores com ela incompatíveis ou quando uma norma especial derroga uma norma geral, situações cuja solução está prevista na Lei de Introdução às Normas do Direito Brasileiro (Decreto-lei 4.657/1942). Da mesma forma, também pode ocorrer que nos conflitos entre regras não seja possível estabelecer-se, com base na data de vigência, qual é a norma aplicável. Exemplo disso ocorre com as causas de exclusão de ilicitude no Código Penal, que estabelecem cláusulas de exceção à incidência das normas primárias que tipificam crimes. Em todos esses casos, deverá o operador do direito buscar uma terceira norma (ainda que implícita) que, regulamentando o conflito, estabeleça qual a solução a ser adotada.

De qualquer forma, seja qual for a norma utilizada para solucionar o conflito entre regras, o resultado do conflito é sempre a delimitação do âmbito de incidência da norma, seja em razão de sua revogação (total ou parcial), seja em razão do estabelecimento de uma cláusula de exceção, de tal sorte que, pelo menos em tese, seria possível considerar que é a partir da solução do conflito que se tem uma visão completa da regra, como se as exceções fossem parte integrante da norma primária.

Em se tratando de colisão entre princípios, entretanto, a solução não passa pelo campo da validade, mediante a revogação ou o estabelecimento de uma cláusula de exceção, mas antes deve ser buscada pela harmonização dos princípios colidentes, pelo balanceamento e ponderação. Com efeito, um princípio é um mandamento de otimização, isto é, trata-se de uma norma que determina que o valor que ele carrega seja aplicado na maior medida possível, de modo que sua aplicação concreta varia de acordo com as circunstâncias fáticas e com os princípios colidentes. Por isso é que, nos casos de colisão de princípios, a solução passa sempre pela verificação, no caso concreto, de qual é a norma resultante do balanceamento[361].

Diversamente do que ocorre com as regras, na colisão de princípios, ambos os princípios colidentes são e continuarão válidos após a resolução do conflito, apenas se buscará, por meio da técnica da ponderação, estabelecer qual será o princípio prevalente naquele caso concreto, o que requer o balanceamento dos valores colidentes, ponderando-se as circunstâncias de modo a possibilitar que, naquelas circunstâncias concretas, seja estabelecido qual é a maior medida possível de aplicação de cada um dos princípios contrapostos, de modo que, para aquele caso, possa ser estabelecido qual princípio deve ceder e em que medida. Atente-se, entretanto, que, como afirma Alexy, isso não implica que o princípio cedente perca sua validade ou que será excepcionado, mas significa unicamente que,

[361] ALEXY, Robert. **Teoria dos direitos fundamentais**.

dadas aquelas circunstâncias concretas, um dos princípios deverá ter precedência em relação ao outro. Alteradas as condições, o resultado do sopesamento também será alterado[362].

Assim, nestes casos, apenas se busca estabelecer uma relação de precedência condicionada, isto é, vinculada às condições fáticas e jurídicas. Esse mesmo tipo de raciocínio se aplica a todas as possíveis colisões de princípios, como aquelas estabelecidas entre a garantia dos direitos fundamentais do acusado e a efetividade da tutela penal.

Os fundamentos teóricos da abordagem principiológica sofreu forte crítica de Habermas, para quem a teoria dos princípios, ao relativizar o caráter deontológico das normas, padeceria de dois graves problemas: o déficit de legitimidade democrática e a perda de força normativa dos princípios e valores. Quanto à primeira questão, afirma Habermas que

> Tal jurisprudência de valores levanta realmente o problema da legitimidade (...) pois ela implica um tipo de concretização de normas que coloca a jurisprudência constitucional no estado de uma legislação concorrente. Perry chega a essa conclusão, reinterpretando arrojadamente os direitos fundamentais, que deixam de ser princípios deontológicos do direito para se tornarem bens teleológicos do direito, formando uma ordem objetiva de valores, que liga a Justiça e o legislador à eticidade substancial de uma determinada forma de vida[363].

De outro lado, quanto às possíveis consequências que a abordagem principiológica acarretaria à normatividade dos princípios, Habermas aponta o risco de que a ponderação acabe por levar a uma relativização de normas, que passarão a ser aplicadas de acordo com as suas finalidades, de tal forma que seria possível que direitos individuais fossem sacrificados em nome de finalidades coletivas, perdendo sua solidez. Alexy resume as críticas feitas por Habermas quanto à insuficiência normativa da tese dos princípios afirmando, no posfácio de 2002 à sua "Teoria dos direitos fundamentais", que, para Habermas[364],

> O caráter principiológico derrubaria um "muro protetor": "se, nos casos de colisão, *todas* as razões puderem adotar caráter de argumentos definidores de finalidades, derruba-se então aquele muros protetor que uma compreensão deontológica das normas introduz no discurso jurídico."
> E o sopesamento de direitos fundamentais não ameaçaria apenas sua força em geral. Ele implicaria também o risco de que os direitos fundamentais fossem vítimas de juízos irracionais,pois não haveria nenhum parâmetro racional para esse sopesamento.

---

[362] CF. ALEXY, Robert. **Teoria dos direitos fundamentais**. p. 93-94.

[363] HABERMAS, Jürgen. **Direito e Democracia: entre faticidade e validade.** Vol. I, Rio de Janeiro: Tempo brasileiro, 2007. p. 320.

[364] ALEXY, Robert. **Teoria dos direitos fundamentais**. p. 576.

Tais críticas, acaso se revelem corretas, terão um efeito demolidor sobre a teoria dos princípios aqui adotada, já que se não houver uma forma racional de efetuar a ponderação, submetendo-a a um controle intersubjetivo, efetivamente estaremos diante de uma tentativa de dar um belo nome a algo que, em última análise, não passa de mais uma forma de decisionismo, o que historicamente sempre se revelou fonte de arbitrariedades e abusos de toda sorte.

Decorre daí que a aceitação da técnica da ponderação depende da possibilidade de que ela seja aplicada de forma racional. É de se ver, entretanto, que não se pode confundir "racionalidade" do discurso jurídico com uma pretensa "objetividade", impossível de ser alcançada. De fato, é verdade que por meio da ponderação não se garante que o resultado em todos os casos sob apreciação do judiciário seja o mesmo. Assim, se a crítica é dirigida a este aspecto, ela é procedente, mas é também absolutamente inócua, já que essa indeterminação do resultado, apesar de ser consideravelmente maior na ponderação, também está presente na subsunção das regras. Na verdade, essa indeterminação do resultado da aplicação das normas aos casos concretos é decorrente da própria natureza interpretativa do Direito, e ela estará presente independentemente do método de aplicação da norma. Com razão, afirma Alexy que

> O simples argumento de que os valores desempenham um papel no sopesamento não constitui uma objeção à possibilidade de fundamentação racional de decisões ponderativas, a não ser que se diga que a argumentação jurídica se torna sempre não-racional ou irracional tão logo se adentre o âmbito das valorações não definidas de forma cogente.

Ocorre que, em toda atividade interpretativa, o campo para a subjetividade do intérprete é sempre muito grande. Aliás, não raro a interpretação de uma regra oferece uma abertura maior à subjetividade do que a ponderação de princípios, bastando que na regra existam conceitos valorativos, de conteúdo indeterminado, nos quais há um imenso espaço para a subjetividade do intérprete na verificação do pressuposto fático necessário para a aplicação de tais regras, posto que, como afirma Hart[365], todo sistema jurídico abre um vasto campo de discricionariedade para os aplicadores do direito tornarem precisos os padrões inicialmente vagos.

Assim, o silogismo com o qual se aplicam as regras, mediante a subsunção dos fatos à interpretação dada à norma, é também uma atividade mental extremamente permeável às

[365] HART, Hebert L. A. **O conceito de direito.** São Paulo: Martins Fontes, 2009. p. 176.

valorações subjetivas feitas pelo aplicador do direito. Na verdade, seja na subsunção das regras, seja na ponderação de princípios, a pretensa objetividade (entendida como previsibilidade absoluta do resultado da interpretação e aplicação do direito) é algo que não existe.

Por isso, desde logo devem ser afastadas as críticas à ponderação relacionadas ao fato desta técnica gerar resultados indeterminados previamente, como se de tal circunstância (verdadeira) pudesse se concluir ser a ponderação um procedimento irracional. Na verdade, uma tal objetividade não só é impossível como é de todo indesejável, pois significaria a instituição de um modelo constitucional em que todas as interpretações possíveis fossem previamente determinadas de modo cogente (única forma concebível de se garantir a objetividade), o que implicaria numa sociedade onde os cidadãos teriam uma margem muito pequena de liberdade e onde o legislativo praticamente seria reduzido à condição de mero executor das decisões previamente adotadas (e esmiuçadas) pelo legislador constituinte, reduzindo a quase nada o espaço democrático de deliberação pelo parlamento, elemento essencial num Estado que se pretenda democrático de direito.

Em todo caso, afastada essa vertente que funda a crítica numa pretensa busca pela objetividade, resta ainda pendente a questão relativa à possibilidade do controle racional da ponderação, condição necessária à legitimidade dessa técnica. Neste ponto, cumpre ressaltar que, para Alexy, a distinção das normas entre regras e princípios, apesar de ser peça fundamental na dogmática dos direitos fundamentais, é ainda insuficiente para garantir a racionalidade nas justificações das decisões jurídicas. Isso porque

> [...] o nível das regras e dos princípios não proporcionam um quadro completo do sistema jurídico. Nem princípios nem regras regulam por si mesmos sua aplicação. Eles representam apenas os pilares passivos do sistema jurídico. Se se quer obter um modelo completo, deve-se agregar aos pilares passivos um ativo, referindo-se ao procedimento de aplicação das regras e princípios. Portanto, os níveis das regras e dos princípios têm de ser completados por um terceiro. Em um sistema orientado por um conceito de razão prática, esse terceiro nível pode ser apenas o de um procedimento que assegure a racionalidade. Dessa maneira, surge um modelo de sistema jurídico que pode ser chamado 'modelo de regras/princípios/procedimento'[366].

[366] ALEXY, Robert**. El concepto y la validez del Derecho**. 2. ed. Barcelona: Gedisa, 1997, p. 173. Tradução nossa. No original: […] el nivel de la regla y el de los principios, no proporciona un cuadro completo del sistema juridico. Ni los principios ni las reglas regulan por si mismos su aplicacion. Ellos representan solo el costado pasivo del sistema juridico. Si se quiere obtener un modelo completo, hay que agregar al costado pasivo uno activo, referido al procedimiento de la aplicacion de las reglas y principios. Por lo tanto, los niveles de las reglas y los principios tienen que ser completados con un tercer nivel. En un sistema orientado por el concepto de la razon practica, este tercer nivel puede ser solo el de un procedimiento que asegure la racionalidad. De esta

Por isso, a tese da ponderação e do balanceamento de princípios como sendo parte de um procedimento racional, sujeito a controle intersubjetivo, pressupõe que sua estrutura seja explicitada, sendo certo que quando se fala em necessidade de garantir a racionalidade da ponderação entre princípios, se está falando também da necessidade de controle racional da restrição aos princípios. Essa ideia tem íntima relação com a noção de proporcionalidade, regra utilizada para controle da legitimidade das restrições aos direitos fundamentais.

Na forma como foi estruturada por Robert Alexy, a regra da proporcionalidade é composta de três sub-regras, que, quando da avaliação de uma restrição a um princípio, devem ser aplicadas sequencialmente para aferir se a restrição é aceitável, isto é, se a restrição é *proporcional*.

Assim, a proporcionalidade, como técnica de controle da racionalidade da restrição aos princípios, deve ser aferida mediante um procedimento sequencial de três etapas: na primeira, afere-se a *adequação* da restrição, isto é, se o sacrifício de um princípio é efetivamente adequado para proteger o outro; em seguida, verifica-se a *necessidade* da restrição, ou seja, se inexiste um outro meio menos gravoso e se a restrição é suficiente; por fim, afere-se a *proporcionalidade em sentido estrito*, quando se efetua a ponderação propriamente dita. As duas primeiras sub-regras (adequação e necessidade) referem-se à avaliação das condições fáticas da realização do princípio, ao passo que última sub-regra (a proporcionalidade em sentido estrito) diz respeito à aferição das condições jurídicas, dado que somente nesta etapa é que se poderá falar em ponderação e balanceamento de princípios colidentes[367].

As três sub-regras da proporcionalidade podem ser tidas como *etapas* necessárias à verificação da legitimidade da restrição ao princípio, posto que sua aplicação é escalonada e subsidiária, ou seja, a verificação da proporcionalidade se dá pela verificação da adequação, necessidade e proporcionalidade em sentido estrito nessa ordem, de maneira sucessiva e subsidiária, de modo que somente quando satisfeita a primeira que se passa à seguinte.

Assim, em primeiro lugar cabe ao intérprete verificar se a restrição é adequada. Se a resposta for negativa (ou seja, caso a restrição não seja apta a realizar o princípio contraposto), desde logo é possível afirmar-se que a restrição não é proporcional, sem

---

manera, surge un modelo de sistema juridico de tres niveles que puede ser llamado "*modelo reglas/principios/procedimiento*

[367] ALEXY, Robert. **La formula del peso.** *In* CARBONELL, Miguel (org.). El principio de proporcionalidad y la interpretación constitucional**.** Quito: Ministerio de Justicia y Derechos Humanos, 2008. p. 15.

necessidade de verificação das outras sub-regras. Portanto, somente após certificar-se que a restrição é adequada é que o intérprete passa à verificação da necessidade da medida, oportunidade em que verificará se ela é suficiente e, ao mesmo tempo, não é excessiva. Novamente, somente caso seja superada esta etapa é que o intérprete passará à fase seguinte, referente à proporcionalidade em sentido estrito.

A adoção da tese de que os princípios são mandamentos de otimização, que determinam sua realização na maior medida possível em face das circunstâncias fáticas e jurídicas, traz consigo a ideia da inexistência de direitos absolutos. De fato, se os direitos fundamentais veiculados pelos princípios são sempre deveres *prima facie*, cujo grau de concretização vai sempre depender não só das condições fáticas concretas, mas também de sua ponderação diante dos princípios contrapostos, tem-se que nenhum direito pode ser tido como absoluto, dado que sempre haverá algum grau de restrição a seu exercício.

Decorre daí que a ponderação vai sempre estar relacionada à definição de qual é a medida correta das restrições aos princípios, já que somente esta espécie de normas tem a dimensão de peso. Por isso, se o que se pretende é estabelecer critérios racionais para a ponderação, faz-se necessário estabelecer de que forma e em que medida as restrições aos princípios são aceitáveis. Essa medida é conferida pelo princípio da proporcionalidade.

Em uma sociedade democrática, há que se buscar o equilíbrio entre os princípios colidentes, estabelecendo proporcionalidade nas suas restrições, não havendo que se falar em supremacia do interesse coletivo (v.g segurança pública) sobre o individual (como a privacidade do investigado) nem tampouco na precedência do individual sobre o coletivo. A dizer, nessa matéria, a solução da questão vai depender de uma análise do caso concreto, com todas as suas nuances e especificidades, sempre buscando harmonizar os princípios colidentes, impondo-se àquele que deve ceder o menor sacrifício possível. Por isso que a regra da proporcionalidade consiste em uma regra de interpretação e aplicação dos direitos voltada a evitar que as restrições impostas aos exercícios de um direito em razão de sua colisão com outro não assumam dimensões desproporcionais[368].

A proporcionalidade é uma técnica de hermenêutica que possibilita concretizar o mandamento de otimização, tutelando cada princípio da melhor maneira possível, ampliando ao máximo suas possibilidades (ou seja, dando concreção ao mandamento de otimização que o princípio encerra) e, ao mesmo tempo, garantindo que os diversos princípios sejam

[368] SILVA, Virgílio Afonso da. **O proporcional e o razoável.** Revista dos Tribunais no. 798, p. 23.

compatíveis entre si. A proporcionalidade, como afirma Miguel Carbonell[369] "constituye hoy en día quizá el más conocido y el más recurrente "límite de los límites" a los derechos fundamentales y en esa medida supone una barrera frente a intromisiones indebidas en el ámbito de los propios derechos".

Resulta daí que a proporcionalidade não é um critério mediante o qual se torna possível verificar a constitucionalidade, a legalidade ou mesmo a legitimidade (jurídica, social, política ou ideológica) de uma norma, mas é a técnica utilizada para aferir a legitimidade de uma dada restrição a um direito fundamental, quando este colide com outro princípio. Somente se pode falar em aplicação da proporcionalidade, portanto, quando se puder identificar de modo claro a prévia existência de princípios colidentes, hipótese em que a solução para a colisão vai se dar na dimensão do peso de cada um desses princípios. Não pode a proporcionalidade, portanto, ser contraposta autonomamente a um princípio ou a uma regra, para afastar sua aplicação.

Essa noção permite evitar um dos maiores riscos ao se tratar de conflitos normativos e aplicação da proporcionalidade, qual seja, o de transforma-la numa "supra-norma", capaz de se sobrepor a qualquer outra norma existente no sistema jurídico, com o agravante de que, fora do contexto de limite às restrições, a proporcionalidade assume uma enorme fluidez, o que acaba permitindo que ela se torne unicamente um recurso de que lança mão o intérprete quando pretender afastar a incidência de uma norma (no mais das vezes uma regra) sem o ônus argumentativo de declarar sua invalidade.

Daí porque é preciso diferenciar claramente as situações em que ocorre verdadeiro conflito normativo (especialmente a colisão entre princípios), daqueles casos em que o que se pretende é tão somente negar validade a uma regra. Com efeito, é comum falar-se em conflito entre uma regra e um princípio quando, em realidade, se está diante de uma restrição ao princípio feita por meio de uma regra. Nas restrições à produção da prova em matéria penal, quase sempre é disso que se cuida, posto que a regra restritiva é produto da ponderação já feita pelo legislador, de modo que essa operação valorativa está, já de início, excluída do campo de atuação do juiz.

De fato, direitos fundamentais, inclusive aqueles relacionados à privacidade, podem e devem ser restringidos por meio de normas constitucionais expressas ou implícitas, bem como por normas infraconstitucionais compatíveis com a Constituição. Do contrário, seria quase

[369] CARBONELL, Miguel. **El principio de proporcionalidad y los derechos fundamentales**. *in* CARBONELL, Miguel (org.). **El principio de proporcionalidad y la interpretación constitucional.** Quito: Ministerio de Justicia y Derechos Humanos, 2008. p. 10.

impossível se pensar na possibilidade de o Estado levar a efeito uma investigação criminal, já que, como afirmado na seção 4.4, a evolução escalonada da persecução penal reflete uma progressiva intervenção sobre a esfera da privacidade.

Assim, em um regime democrático, é papel a ser precipuamente desempenhado pelo legislador a restrição de direitos fundamentais por meio do estabelecimento de regras. Nesse sentido, tem-se que o legislador, ao atuar restringindo a privacidade e regulamentando a forma como a prova deve ser colhida, estabelece limites que servem para o exercício da privacidade, e, também, para a sua restrição.

O legislador, ao estabelecer proibições ou requisitos para a produção da prova tendo em vista a proteção à privacidade e à intimidade, mesmo que fora da esfera especificamente penal (vg, em matéria fiscal ou empresarial), estabelece também limites extrínsecos à produção da prova, em nome da tutela da privacidade e, assim agindo, não está propriamente estabelecendo uma ponderação entre os princípios da privacidade e da segurança pública, mas antes está restringindo, através de uma regra, o princípio da privacidade, estabelecendo seus contornos e conformando o campo legítimo do seu exercício.

De fato, é até possível imaginar-se hipóteses de colisões entre regras e princípios (caso em que, segundo Alexy, a solução passa pela ponderação entre o princípio e o princípio que dá suporte à norma contraposta[370]). Entretanto, na vasta maioria dos casos em que aparentemente se está diante de um conflito entre um princípio e uma regra, na realidade o que se verifica é unicamente uma restrição ao princípio por meio da regra, feita a partir de um sopesamento realizado pelo legislador e que gerou a restrição ao princípio[371]. Mais uma vez recorrendo ao exemplo da interceptação telefônica, é o que ocorre quando o legislador estabeleceu que a interceptação "[...] não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova." (art. 5º). Nesse caso, o prazo de 15 dias e a possibilidade de renovação são restrições à privacidade, ao passo que a necessidade de que, para a renovação, seja necessária a comprovação da indispensabilidade da medida configura uma restrição à busca pela verdade na tutela da segurança pública, caso em que concretamente a proteção da privacidade atua como limite extrínseco à produção da prova. Neste exemplo, todas essas restrições configuram limitações feitas pelo legislador quando da concretização do direito constitucional que dá suporte à norma e não ensejam a possibilidade de se ponderar se devem ou não ser aplicados.

---

[370] Cf. ALEXY, Robert. **Teoria dos direitos fundamentais**. p. 90, nota 24.

[371] SILVA, Virgílio Afonso da. **Direitos fundamentais. Conteúdo essencial, restrições e eficácia.** p. 52.

Naquelas nas hipóteses em que o legislador, no exercício de sua função própria de conformação dos princípios constitucionais, cria regras que restringem direitos fundamentais, ele já está fazendo de antemão um sopesamento entre os princípios colidentes e esse primeiro juízo de ponderação do legislador não é propriamente uma aplicação da regra da proporcionalidade. Esta somente terá lugar num segundo momento, quando se for verificar concretamente se a restrição estabelecida é legítima.

Por isso é que se torna imperioso compreender o que efetivamente significa afirmar que a privacidade é um limite extrínseco à produção da prova penal. A proteção constitucional à "intimidade, a vida privada, a honra e a imagem", a inviolabilidade de domicílio e o sigilo de dados e das comunicações representam um limite à busca da verdade, o que na *Common Law* se denomina *privilege.* Evidentemente esse limite não é absoluto, já que há relevantes razões de interesse público que justificam sua restrição pelo legislador, no exercício de sua competência constitucional de conformação da constituição por meio do estabelecimento de restrições a direitos fundamentais.

Nesse sentido, bastante elucidativas são as considerações feitas pelo Ministro Edson Fachin em seu voto na ADI 5642, na qual a Associação Nacional das Operadoras de Celulares (ACEL) questiona a constitucionalidade do art. 11 da Lei 13.344/2016, que dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas, e inclui os arts. 13- A e 13-B ao Código de Processo Penal, que conferem a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial.

Em seu voto, o relator, Ministro Edson Fachin, após ressaltar que o objeto da ADI tornava necessária uma atualização da cláusula constitucional da proteção da privacidade para a era digital, e que a Constituição prevê expressamente que somente a lei pode estabelecer, mediante autorização judicial, restrições ao sigilo das comunicações, afirmou que

> O sigilo é necessário porque ele ampara uma legítima expectativa de privacidade não apenas no sentido de ser deixado a sós, como defendia o Justice Brandeis, mas sobretudo para proteger escolhas de vida contra o controle estatal e a estigmatização social (RODOTÀ, Stefano. General Presentation of Problems related to Transsexualism. In: Transsexualism, Medicine and Law: Proceedings of the XXIIIrd Colloquy on European Law. Strasbourg: Concil of Europe Publishing, 1995. p. 22-23).
>
> O direito à proteção da privacidade não é absoluto, mas qualificado. A lei pode restringir esse direito ao prever as hipóteses em que o Poder Judiciário poderá afastá-lo e a finalidade para a qual a restrição é admitida é a de investigar as infrações à lei, pois as provas das infrações raramente ficam disponíveis publicamente[372]

Esse trecho do voto é relevante pois articula dois elementos essenciais para a compreensão da privacidade digital em matéria penal: em primeiro lugar, ele ressalta o caráter contextual da privacidade em matéria penal, que deve atender às razoáveis expectativas sociais acerca do equilíbrio entre a proteção ao indivíduo e a efetividade das investigações. A rigor, aquilo que o Ministro denomina de "legítimas expectativas de privacidade" constituem exatamente aquilo a que Nissenbaum se refere como normas sociais que conformam o direito de privacidade e que possibilitam sua aderência ao momento histórico e às opções jurídico-políticas da sociedade. Essa conformação social, quando utilizada para a análise da legitimidade de uma restrição à privacidade, se traduz no processo por meio de uma justificação adequada, que possibilita o controle intersubjetivo por meio dos recursos. A dizer, é o procedimento adotado, aliado à argumentação, que possibilita o controle da racionalidade da decisão acerca da legitimidade da restrição.

Em segundo lugar, ao ressaltar que o direito à privacidade não é absoluto, mas qualificado, a decisão destaca a possibilidade de que a privacidade seja objeto de ponderação e balanceamento diante de um caso concreto para aferir a legitimidade da restrição, além de deixar explícito que, na ponderação com outros valores, a privacidade parte de uma posição de destaque, com um grande peso relativo.

Nesse ponto, vale ressaltar que o direito brasileiro há muito já convive com a possibilidade de acesso a dados cadastrais sem ordem judicial, como aquela prevista no caso da quebra de sigilo bancário pela autoridade fazendária, previsto na Lei Complementar 105/2001, possibilidade que foi declarada constitucional pelo Supremo Tribunal Federal na ADI 2.858, relatada pelo Ministro Dias Toffoli e julgada pelo Pleno do Supremo em 20/10/2016. Naquela oportnidade, o Supremo Tribunal Federal entendeu que, uma vez que o

[372] BRASIL. SUPREMO TRIBUNAL FEDERAL. **ADI 5642.** Voto do Ministro Luiz Edson Fachin. Disponível em https://www.conjur.com.br/dl/voto-fachin-uso-dados.pdf

artigo 6º da LC 105 dispõe que as informações bancárias transferidas ao Fisco serão mantidas em sigilo, sob pena de responsabilização cível e criminal, a obtenção de dados bancários diretamente pelo Fisco não se trata propriamente de uma quebra de sigilo, mas mera transferência de sigilo bancário ao ente público que já é obrigado a assegurar o sigilo fiscal. Assim, as informações que antes eram protegidas pela instituição financeira passarão a ser protegidas pelo Fisco. No julgamento da ADI, o STF fez uma ponderação entre a proteção à privacidade do contribuinte e o interesse público relativo ao combate à sonegação fiscal e à possibilidade de o Estado obter recursos para cumprir seus deveres prestacionais. O julgamento da referida ADI foi assim ementado:

> EMENTA Ação direta de inconstitucionalidade. Julgamento conjunto das ADI nº 2.390, 2.386, 2.397 e 2.859. Normas federais relativas ao sigilo das operações de instituições financeiras. Decreto nº 4.545/2002. Exaurimento da eficácia. Perda parcial do objeto da ação direta nº 2.859. Expressão "do inquérito ou", constante no § 4º do art. 1º, da Lei Complementar nº 105/2001. Acesso ao sigilo bancário nos autos do inquérito policial. Possibilidade. Precedentes. Art. 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentadores. Ausência de quebra de sigilo e de ofensa a direito fundamental. Confluência entre os deveres do contribuinte (o dever fundamental de pagar tributos) e os deveres do Fisco (o dever de bem tributar e fiscalizar). Compromissos internacionais assumidos pelo Brasil em matéria de compartilhamento de informações bancárias. Art. 1º da Lei Complementar nº 104/2001. Ausência de quebra de sigilo. Art. 3º, § 3º, da LC 105/2001. Informações necessárias à defesa judicial da atuação do Fisco. Constitucionalidade dos preceitos impugnados. ADI nº 2.859. Ação que se conhece em parte e, na parte conhecida, é julgada improcedente. ADI nº 2.390, 2.386, 2.397. Ações conhecidas e julgadas improcedentes. 1. Julgamento conjunto das ADI nº 2.390, 2.386, 2.397 e 2.859, que têm como núcleo comum de impugnação normas relativas ao fornecimento, pelas instituições financeiras, de informações bancárias de contribuintes à administração tributária. 2. Encontra-se exaurida a eficácia jurídico-normativa do Decreto nº 4.545/2002, visto que a Lei n º 9.311, de 24 de outubro de 1996, de que trata este decreto e que instituiu a CPMF, não está mais em vigência desde janeiro de 2008, conforme se depreende do art. 90, § 1º, do Ato das Disposições Constitucionais Transitórias -ADCT. Por essa razão, houve parcial perda de objeto da ADI nº 2.859/DF, restando o pedido desta ação parcialmente prejudicado. Precedentes. 3. A expressão "do inquérito ou", constante do § 4º do art. 1º da Lei Complementar nº 105/2001, refere-se à investigação criminal levada a efeito no inquérito policial, em cujo âmbito esta Suprema Corte admite o acesso ao sigilo bancário do investigado, quando presentes indícios de prática criminosa. Precedentes: AC 3.872/DF-AgR, Relator o Ministro Teori Zavascki, Tribunal Pleno, DJe de 13/11/15; HC 125.585/PE-AgR, Relatora a Ministra Cármen Lúcia, Segunda Turma, DJe de 19/12/14; Inq 897-AgR, Relator o Ministro Francisco Rezek, Tribunal Pleno, DJ de 24/3/95. 4. Os artigos 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentares (Decretos nº 3.724, de 10 de janeiro de 2001, e nº 4.489, de 28 de novembro de 2009) consagram, de modo expresso, a permanência do sigilo das informações

> bancárias obtidas com espeque em seus comandos, não havendo neles autorização para a exposição ou circulação daqueles dados. Trata-se de uma transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo, permanecendo resguardadas a intimidade e a vida privada do correntista, exatamente como determina o art. 145, § 1º, da Constituição Federal. 5. A ordem constitucional instaurada em 1988 estabeleceu, dentre os objetivos da República Federativa do Brasil, a construção de uma sociedade livre, justa e solidária, a erradicação da pobreza e a marginalização e a redução das desigualdades sociais e regionais. Para tanto, a Carta foi generosa na previsão de direitos individuais, sociais, econômicos e culturais para o cidadão. Ocorre que, correlatos a esses direitos, existem também deveres, cujo atendimento é, também, condição sine qua non para a realização do projeto de sociedade esculpido na Carta Federal. Dentre esses deveres, consta o dever fundamental de pagar tributos, visto que são eles que, majoritariamente, financiam as ações estatais voltadas à concretização dos direitos do cidadão. Nesse quadro, é preciso que se adotem mecanismos efetivos de combate à sonegação fiscal, sendo o instrumento fiscalizatório instituído nos arts. 5º e 6º da Lei Complementar nº 105/ 2001 de extrema significância nessa tarefa. 6. O Brasil se comprometeu, perante o G20 e o Fórum Global sobre Transparência e Intercâmbio de Informações para Fins Tributários (Global Forum on Transparency and Exchange of Information for Tax Purposes), a cumprir os padrões internacionais de transparência e de troca de informações bancárias, estabelecidos com o fito de evitar o descumprimento de normas tributárias, assim como combater práticas criminosas. Não deve o Estado brasileiro prescindir do acesso automático aos dados bancários dos contribuintes por sua administração tributária, sob pena de descumprimento de seus compromissos internacionais. 7. O art. 1º da Lei Complementar 104/2001, no ponto em que insere o § 1º, inciso II, e o § 2º ao art. 198 do CTN, não determina quebra de sigilo, mas transferência de informações sigilosas no âmbito da Administração Pública. Outrossim, a previsão vai ao encontro de outros comandos legais já amplamente consolidados em nosso ordenamento jurídico que permitem o acesso da Administração Pública à relação de bens, renda e patrimônio de determinados indivíduos. 8. À Procuradoria-Geral da Fazenda Nacional, órgão da Advocacia-Geral da União, caberá a defesa da atuação do Fisco em âmbito judicial, sendo, para tanto, necessário o conhecimento dos dados e informações embasadores do ato por ela defendido. Resulta, portanto, legítima a previsão constante do art. 3º, § 3º, da LC 105/2001. 9. Ação direta de inconstitucionalidade nº 2.859/DF conhecida parcialmente e, na parte conhecida, julgada improcedente. Ações diretas de inconstitucionalidade nº 2390, 2397, e 2386 conhecidas e julgadas improcedentes. Ressalva em relação aos Estados e Municípios, que somente poderão obter as informações de que trata o art. 6º da Lei Complementar nº 105/2001 quando a matéria estiver devidamente regulamentada, de maneira análoga ao Decreto federal nº 3.724/2001, de modo a resguardar as garantias processuais do contribuinte, na forma preconizada pela Lei nº 9.784/99, e o sigilo dos seus dados bancários.
> (STF - ADI 2859, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 24/02/2016, ACÓRDÃO ELETRÔNICO DJe-225 DIVULG 20-10-2016 PUBLIC 21-10-2016)

Em seguida, o STF enfrentou essa mesma questão no julgamento do RE 601.314, relatado pelo Min. Edson Fachin e julgado sob o rito da repercussão geral (Tema 225),

assentando a seguinte tese: “o 6º da Lei Complementar 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o translado do dever de sigilo da esfera bancária para a fiscal”. Naquele julgamento, o Ministro Barroso deixou expresso em seu voto o raciocínio de balanceamento e ponderação realizado:

> Em relação à adequação da medida, é preciso verificar se o acesso direto aos dados bancários dos contribuintes por parte da Administração Tributária é um meio idôneo para alcançar os fins pretendidos. Isto é, se as restrições impostas aos direitos fundamentais dos contribuintes são aptas a promover os interesses contrapostos de permitir que a fiscalização promova um combate eficaz aqueles contribuintes que buscam sonegar tributos, omitir receitas, ocultar patrimônio e dar curso à evasão de fiscal. Nesse sentido, entendo ser fora de dúvidas que um instrumento que imponha às instituições financeiras, e não ao contribuinte eventualmente interessado em se esquivar do pagamento, a obrigação de prestar as informações que podem levar a efetiva apuração do valor devido dos tributos, **é um mecanismo com aptidão de promover a finalidade de combater as mais diversas formas de fuga ilegítima da tributação e controlar o fluxo de capitais, inclusive, para fins penais** (grifamos)

Esse entendimento foi posteriormente ampliado no âmbito do Superior Tribunal de Justiça, que autorizou o acesso das informações fiscais às requisições feitas pelo Ministério Público, sob o fundamento de que constituiriam apenas “dados cadastrais”, insuscetíveis de revelar informações sensíveis da vida privada de seus titulares e que, por isso, não seriam abrangidos pela proteção da reserva de jurisdição constante do inciso XII do art. 5º da Constituição Federal. Nesse ponto, por sua pertinência para a discussão, vale transcrever a ementa do *leading case* no STJ acerca da possibilidade de requisição direta de dados cadastrais pelo Ministério Público:

> PROCESSUAL CIVIL. AÇÃO CIVIL PÚBLICA. LEGITIMIDADE DO MINISTÉRIO PÚBLICO. FORNECIMENTO DE DADOS CADASTRAIS DE CLIENTES DE INSTITUIÇÕES FINANCEIRAS MEDIANTE REQUISIÇÃO DIRETA DO PARQUET OU DA POLÍCIA FEDERAL. DIREITOS DIFUSOS E COLETIVOS CARACTERIZADOS.SEGURANÇA PÚBLICA. ACESSO A DADOS CADASTRAIS. POSSIBILIDADE. HISTÓRICO DA DEMANDA 1. Tratam os presentes autos de Ação Civil Pública proposta pelo Ministério Público Federal buscando, em síntese, "assegurar o fornecimento de informações constantes dos cadastros de clientes em instituições financeiras (nome completo, endereço, telefone, e-mail, número de documentos, etc.), quando requisitadas por seus membros para instruir processo judicial, inquérito policial ou qualquer outro procedimento de investigação criminal ou civil, e por Delegados de Polícia Federal, para instruir inquérito policial devidamente formalizado" (fl. 1.106, e-STJ).2.. O Tribunal regional

consignou (fl. 1.108-1.109, e-STJ): "Não se desconhece a existência de decisões judiciais favoráveis à tese defendida pelo autor da ação, decisões que aceitam o uso da ação civil pública como meio para facilitar ou aprimorar a atuação do próprio Ministério Público Federal (...). Entendo, porém, que a questão passa pela natureza da legitimação do Ministério Público para a ação civil pública. Na defesa dos interesses tuteláveis pela ação civil pública, o Ministério Público atua em nome próprio na defesa de interesses de terceiros amparado, neste aspecto, expressamente pela ordem jurídica. A defesa dos interesses sociais e individuais indisponíveis é, até, uma de suas funções institucionais (artigo 127, CF), razão pela qual, na ação civil pública, sua legitimação é extraordinária. (...) Alega-se a defesa de interesse difuso, mas como restou bem delineado acima, de interesse difuso não se trata, mas de interesse do próprio Parquet". LEGITIMIDADE ATIVA DO MINISTÉRIO PÚBLICO FEDERAL 3. A pretensão deduzida na presente Ação Civil Pública busca a tutela da segurança pública, interesse difuso de natureza indisponível. Assim, a legitimação ativa do Parquet Federal mostra-se evidente, nos termos do art. 25, IV, da Lei 8.625/1993. O caráter difuso do direito à segurança pública foi considerado pelo STF ao reconhecer a legitimidade do Ministério Público Federal para ajuizamento de Ação Civil Pública, ainda que analisada sob enfoque distinto, in verbis: STF, AgR no RE 367.432/PR, Rel. Min. Eros Grau, Segunda Turma, DJe 13.5.2010, publicado em 14.5.2010. MÉRITO DA CONTROVÉRSIA 4. **O Ministério Público, em suas atividades precípuas, depara-se constantemente com a necessidade de buscar dados e informações de usuários investigados para instruir processo judicial, inquérito policial ou qualquer outra investigação criminal ou civil, constantes em bancos de dados de pessoas jurídicas de direito público ou privado. O acesso a tais bancos é essencial para que haja sucesso na tarefa de individualização e identificação de agentes praticantes das mais diversas infrações penais, seja na posição de autores, partícipes ou até mesmo como testemunhas de crimes.** 5. Outro ponto imprescindível ao deslinde da presente controvérsia é a distinção de dados e dados cadastrais. **Enquanto os "dados" revelam aspectos da vida privada ou da intimidade do indivíduo e possuem proteção constitucional esculpida no art. 5º, X e XII, da Constituição Federal, os "dados cadastrais" se referem a informações de caráter objetivo que todos possuem, não permitindo a criação de qualquer juízo de valor sobre o indivíduo a partir de sua divulgação.** São essencialmente um conjunto de informações objetivas fornecidas pelos consumidores/clientes/usuários sistematizadas em forma de registro de fácil acesso por meio de seu armazenamento em banco de dados de pessoas jurídicas de direito público ou privado, contendo informações como nome completo, CPF, RG, endereço, número de telefone etc. 6. **O Supremo Tribunal Federal consolidou jurisprudência de que o conceito de "dados" previsto na Constituição é diferente do de "dados cadastrais". Somente aquele tem assegurada a inviolabilidade da comunicação de dados. A propósito: STF, RE 418.416/SC, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, DJ 19.12.2006; STF, HC 91.867/PA, Rel. Min. Gilmar Mendes, Segunda Turma, DJe 19.9.2012, publicado em 20.9.2012. 7. Os dados cadastrais bancários (informações de seus correntistas tais como número da conta-corrente, nome completo, RG, CPF, número de telefone e endereço) estão incluídos na definição de dados cadastrais e não estão, portanto, protegidos por sigilo bancário, que abriga apenas os serviços da conta (aplicações, transferências, depósitos e etc) e não os dados cadastrais de seus usuários.** 8. Ressalte-se que o STJ, ao apreciar controvérsia referente ao

acesso a dados cadastrais telefônicos, adotou o mesmo entendimento aqui esposado, ao consignar que informações referentes ao proprietário de linha telefônica (nome completo, CPF, RG, número da linha e endereço) buscam somente a identificação de seus usuários e, portanto, não estão acobertadas pelo sigilo das comunicações telefônicas. Nesse sentido: RHC 82.868/MS, Rel. Ministro Felix Fischer, Quinta Turma, DJe 1º.8.2017; HC 131.836/RJ, Rel. Ministro Jorge Mussi, Quinta Turma, DJe 6.4.2011. ALEGAÇÃO DE PERDA SUPERVENIENTE DO INTERESSE DE AGIR 9. Destaque-se que, na sustentação oral procedida pelo procurador da parte recorrida, Itaú Unibanco S.A., na sessão de julgamento realizada no dia 10.4.2018, bem como nos memoriais entregues, foi levantada a questão de possível perda superveniente do interesse de agir, ante a mudança no quadro normativo que rege a matéria a partir da edição de duas leis. 10. Inicialmente, ressalte-se que ambas as leis invocadas (Leis 12.683/2012 e 12.850/2013) já se encontravam em vigor quando do pronunciamento judicial do Tribunal a quo no acórdão que ensejou o presente Recurso Especial. Todavia, os mencionados dispositivos legais não foram analisados pela instância de origem. Ausente, portanto, o requisito do prequestionamento, o que atrai, por analogia, o óbice da Súmula 282/STF. O Superior Tribunal de Justiça entende que, em razão da falta de prequestionamento, a alegação de existência de fato superveniente é obstada na via especial. 11. Ademais, os enunciados normativos apontados versam sobre procedimentos específicos e mais restritos do que o objeto desta Ação Civil Pública: a Lei 9.613/1998 trata dos crimes de "lavagem" ou ocultação de bens, direitos e valores, ao passo que a Lei 12.850/2013 é referente a organização criminosa, meios de obtenção de prova, infrações correlatas e procedimento criminal. Assim, percebe-se que a legislação diz respeito a procedimentos específicos de atuação da legislação penal e processual penal, não se podendo falar em perda superveniente do interesse de agir do Parquet na presente Ação. 12. Além disso, ainda que se afastasse tal óbice, destaque-se que o art. 17-B da Lei 9.613/1998, incluído pela Lei 12.683/2012, e o art. 15 da Lei 12.850/2013, na verdade, reforçam a tese argumentativa do provimento do presente apelo recursal. Ambos indicam a possibilidade de a autoridade policial e de o Ministério Público terem acesso, independentemente de autorização judicial, de dados cadastrais do investigado para fins investigatórios, em total harmonia ao que se pleiteia no presente Recurso Especial. NÃO INCIDÊNCIA DO PRECEDENTE FIRMADO NO RESP 1.611.821/MT 13. Inaplicável o precedente invocado pela parte recorrida, Caixa Econômica Federal, em sua sustentação oral, firmado no julgamento do REsp 1.611.821/MT, de relatoria do Ministro Marco Aurélio Bellizze, realizado pela Terceira Turma do STJ em 13.6.2017, por se tratar de questão distinta da que está sendo debatida nos presentes autos. Naquela ocasião, a controvérsia abordava questões ligadas à "divulgação de operações passivas e ativas dos clientes, ainda que se dispense a indicação de valores financeiros", em que se buscava "a relação nominal de clientes que contrataram determinadas operações num período temporal determinado, situação que se encaixa com perfeição no dever de sigilo definido na legislação complementar específica", enquanto os presentes autos tratam unicamente do acesso a dados cadastrais não abrangidos pela proteção constitucional. CONCLUSÃO 14. Finalmente, destaque-se que os precedentes firmados no Supremo Tribunal Federal, no julgamento das ADIs 2390, 2386, 2397 e 2859 e do Recurso Extraordinário 601.314, não se aplicam aos presentes autos, uma vez que tratava de controvérsia distinta - o sigilo bancário - e não de acesso a dados cadastrais, estes últimos não abarcados pela proteção constitucional, **embora naquela ocasião tenha sido**

> **reconhecida a constitucionalidade da LC 105/2001, que permite à Receita Federal receber dados bancários de contribuintes fornecidos diretamente pelos bancos, sem prévia autorização judicial. 15. Ao Ministério Público deve ser assegurado o acesso a informações não agasalhadas por sigilo bancário (dados cadastrais de pessoas investigadas), para o fim de instruir os procedimentos investigatórios de natureza penal e civil.** 16. Recurso Especial provido, devolvendo ao Tribunal de origem para que prossiga com a Ação. (STJ - REsp 1561191/SP, Rel. Ministro HERMAN BENJAMIN, SEGUNDA TURMA, julgado em 19/04/2018, DJe 26/11/2018 - grifamos)

A análise deste precedente indica a adoção de uma concepção da privacidade ligada ao limite de acesso a dados pessoais (privacidade como acesso), seguido de uma ponderação entre privacidade e segurança que se valeu de precedentes do Supremo os quais adotam uma distinção entre dados cadastrais e dados constitucionalmente protegidos que talvez não mais se mostre adequada para a realidade contemporânea, em que a capacidade de processamento e o *big data* permitem o estabelecimento de correlações aptas a gerar dados sensíveis do indivíduo investigado a partir de meros fragmentos de informações que ele compartilha. Os dados cadastrais, nesse contexto, tornam-se valiosas fontes de dados pessoais sensíveis, não podendo ser caracterizados como meras informações cuja transferência não vulneraria sequer a cláusula constitucional de reserva de jurisdição.

De qualquer sorte, para fins da análise aqui empreendida, cumpre notar que, no quadro constitucional desenhado a partir das decisões do STF e do STJ acerca da distinção entre dados de comunicação e dados cadastrais, entendeu o Ministro Fachin, ao proferir seu voto na já mencionada ADI 5642, que o sentido da expressão "dados cadastrais" foi levado em conta pelo Poder Legislativo nas alterações feitas à lei processual penal, quando ampliou os poderes de investigação das autoridades policiais e dos membros do Ministério Público. Na realidade, esse quadro conceitual, para além de resguardar a restrição à privacidade feita pelo legislador, contribuiu para, nas palavras do Ministro, "afastar a expectativa de privacidade que esses dados cadastrais teriam quando dispôs sobre a obrigatoriedade de seu fornecimento."

A avaliação da expectativa legítima de privacidade é o que garante que se possa efetuar uma análise correta das restrições à privacidade no âmbito penal. De fato, para além da análise e ponderação feita pelo legislador quando estabelece as regras legais para a produção da prova, também o aplicador do direito é chamado a analisar se concretamente, naquele caso específico, a restrição autorizada pela lei é legítima e proporcional. Para isso, a abordagem mais adequada para a correta compreensão da privacidade em toda sua complexa multidimensionalidade é a adoção de uma concepção contextual da privacidade, que, aliada ao princípio da proporcionalidade, permitam otimizar a colisão entre a proteção do indivíduo

e a proteção da coletividade, ponderando e balanceando as restrições que a tutela da segurança pública impõe à privacidade.

Essa abordagem traz como grande vantagem possibilitar uma abertura às constantes alterações das normas sociais que regem as expectativas legítimas da sociedade quanto à proteção da privacidade, ao mesmo tempo em que possibilita o controle intersubjetivo da racionalidade da argumentação utilizada para justificar a prevalência de uma ou outra posição acerca da melhor solução à colisão. Nesse aspecto, vale ressaltar que essa maleabilidade e abertura foi bem percebida pelo Ministro Fachin em seu voto, quando, ao apreciar a posição do STF quanto à distinção entre dados e dados cadastrais, afirmou:

> [...] na era digital, são no mínimo discutíveis a aplicação do conceito de "dados cadastrais" para definir o alcance dos poderes de requisição sem mandado judicial por parte das autoridades policiais e do Ministério Público. Por isso, apesar de a redação legislativa contida no art. 13-A do Código de Processo Penal limitar-se a "dados e informações cadastrais", expressão consagrada na jurisprudência deste Tribunal, é preciso não colocá-la acima da própria proteção constitucional, isto é, não se deve interpretar a expressão de modo a tornar ineficaz a proteção constitucional.
> Como advertem Dennys Antonialli e Jacqueline de Souza Abreu (Brazil and the Treasure Trove's Tales: A Study on the Evolution and Popularization of Phones and Law Enforcement Access to Communications. In: FELSBERGER, Stefanie; SUBRAMANIAN, Ramesh. Mobile Technology and Social Transformation. Abingdon: Routledge, 2021, tradução livre):
>
> > Na prática, essas autoridades [delegados de polícia e membros do Ministério Público] utilizam esses dispositivos legais [que lhes atribuem o poder de requisição de dados cadastrais] para justificar a requisição de dados a empresas de telefonia em todos os casos; e a questão só é levada às cortes para revisão se uma empresa se recusar a cumprir. A falta de qualquer critério formal ou material para o fornecimento de informações deixa esses procedimentos ainda mais discricionários.
>
> Por tudo isso, este Tribunal não pode aceitar acriticamente a utilização da expressão "dados e informações cadastrais" para reconhecer como legítima toda e qualquer interferência no direito à privacidade, já que a atual capacidade de produção e análise de dados, ainda que mais simples e públicos, pode trazer significativos impactos.

Segundo o entendimento do relator, apesar da restrição à privacidade que a lei autoriza ser potencialmente grave, o fato de a situação regulada ser de especial gravidade e de a repressão a esse crime exigir uma ação rápida e efetiva para proteger a vida e a incolumidade física da vítima, fazem com que a restrição imposta pelo legislador seja se torne proporcional. Com efeito, segundo o Ministro Fachin, "não deve haver expectativa de privacidade para

quem está em situação de flagrante delito de crime grave com vítimas submetidas à restrição de liberdade.”

Outra questão relativa à ponderação da privacidade de dados com as necessidades de instrução criminal foi decidida de modo similar pelo STF no julgamento do RE 1.055.941, sob o regime da repercussão geral, no qual se discutia a possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte, obtidos pela Receita Federal no legítimo exercício de seu dever de fiscalizar, sem autorização prévia do Poder Judiciário. O acórdão foi assim ementado

> Ementa Repercussão geral. Tema 990. Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.(RE 1055941, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 04/12/2019, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO PUBLIC 06-10-2020)

Cabe salientar que, nesse caso, o Instituto Brasileiro de Ciências Criminais - IBCCRIM, atuando como *amicus curiae*, sustentou a tese de que, nada obstante o STF já ter decidido que é legítima a circulação de dados bancários sigilosos entre entes da administração para fins fiscais ou dos informes da Unidade de Inteligência Financeira (UIF) entre órgãos da administração, porque se estaria tratando, em suma, de transferência de sigilo, o mesmo argumento não valeria para autorizar a transferência de tais dados para o Ministério Público para fins de persecução penal, dado que o Estado-administrador não se confunde com o Estado-persecutório.

O relator, Ministro Dias Toffoli, inicialmente havia reconhecido a possibilidade de que o compartilhamento de dados bancários e fiscais dos órgãos administrativos de fiscalização e controle com o Ministério Público pudessem caracterizar ofensa às matrizes constitucionais

da intimidade e do sigilo de dados (art. 5º, incisos X e XII, da CF), tendo determinado a suspensão dos processos judiciais em andamento e inquéritos em trâmite em que essa questão estivesse sendo discutida.

No julgamento do recurso, entretanto, a partir do voto do Ministro Alexandre de Moraes, a propalada distinção entre a atividade meramente administrativa e a atividade persecutória não foi acolhida. O Ministro sustentou que, tendo sido declaradas lícitas as provas obtidas pela Receita e pela UIF, colhidas em absoluto respeito ao direito processual e material, nos termos da legislação declarada constitucional pelo STF (LC 105), não se poderia impedir que tais elementos fossem encaminhados ao titular da ação penal. Nas palavras do Ministro Alexandre de Moraes[373],

> Não permitir o compartilhamento da íntegra do procedimento fiscalizatório, com todos os dados fiscais e bancários, que constitucionalmente esse órgão pode juntar no procedimento administrativo tributário, dos quais depende o Ministério Público para atuar, parece-me atentar contra todo o mecanismo legal de relativização do sigilo financeiro para o combate à criminalidade
> [...]
> Os direitos e garantias individuais, portanto, não podem ser utilizados como um verdadeiro escudo protetivo da prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil, tributária ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito

Esse entendimento foi seguido pelo Relator, Ministro Dias Toffoli, que os incorporou a seu voto para formular as teses aprovadas pelo Plenário. Também nesse julgamento se evidencia não só o papel de enorme relevância que as cláusulas constitucionais de proteção à privacidade desempenham no âmbito penal, na medida em que impõem limites à atuação dos entes estatais encarregados da persecução penal, mas também evidencia que o contexto em que a informação pessoal será utilizada é de suma importância para a avaliação da legitimidade da intromissão estatal na esfera privada do indivíduo.

Essa circunstância também foi percebida na apreciação da possibilidade de os relatórios de inteligência produzidos pela UIF fossem compartilhados. Nesse tópico, o STF lançou mão de uma concepção de privacidade restrita à dimensão individual do controle de acesso para avaliar se o fornecimento de tais informações representaria uma lesão desproporcional à intimidade dos investigados, avaliando a legitimidade da restrição imposta pelo legislador sem levar em consideração, pelo menos de forma expressa, qualquer distinção

[373] BRASIL. STF. **RE 1.055.941/SP.** Plenário. Rel. Ministro Dias Toffoli, julgado em 04.12.2019. Inteiro teor disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755364496

contextual decorrente da mudança da finalidade para a qual seria utilizada a informação, tendo validado sua utilização unicamente baseado no fato de que, nos termos do voto do relator[374],

> [...] os relatórios de inteligência disseminados pela UIF, repito, "não t[ê]m por finalidade fornecer um extrato completo de transações de um determinado cliente ou conjunto de clientes", mas tão somente a função de "'chamar a atenção para certas transações[,] contrapartes ou situações que foram consideradas atípicas ou suspeitas" (Petição/STF nº 69.779/19 – grifos nossos) Dessa perspectiva, por entender preservada a intangibilidade da intimidade e do sigilo de dados, que gozam de proteção constitucional (art. 5º, incisos X e XII, da CF), não há dúvidas, para mim, quanto a possibilidade de a UIF compartilhar relatórios de inteligência (RIF por intercâmbio) por solicitação do Ministério Público, da polícia ou de outras autoridades competentes

Ainda que tenha sido expressamente afirmada no voto a necessária distinção entre atividade de inteligência e prova para instrução criminal, ressaltando-se que a "Unidade de Inteligência brasileira, [...] simplesmente produz atividade de inteligência, sem, contudo, certificar a legalidade ou não das operações financeiras analisadas", o fato é que, como já afirmado, a realidade contemporânea da massiva utilização de *Big data* para coletar e processar tais dados tornam a ideia de que os dados coletados são meros fragmentos de informação sem aptidão para vulnerar a privacidade não parece ser o caminho mais adequado para se pensar a privacidade na era digital.

Vale ressaltar que não se discute aqui o resultado da argumentação, mas o procedimento de justificação adotado, que deixou de levar em consideração o contexto de produção e de utilização da informação, sendo certo que seria possível se alcançar a mesma decisão, com ganhos de segurança jurídica, através de uma argumentação que acolhesse a tese do IBCCRIM, de diferenciação entre o Estado-administração e o Estado persecução para estabelecer de modo mais claro os limites da atuação dos órgãos de persecução penal no que toca ao acesso a dados dos investigados.

Nesse sentido, bem representativa de como a adoção de uma concepção restrita da privacidade pode contribuir para que as discussões permaneçam inconclusas, recentemente a Terceira Seção do Superior Tribunal de Justiça, decidiu, por maioria, que a tese firmada no Tema 990 da repercussão geral do STF somente é válida para o encaminhamento de representação fiscal para fins penais, não autorizando que a requisição seja feita diretamente

[374] BRASIL. STF. **RE 1.055.941/SP.** Plenário. Rel. Ministro Dias Toffoli. julgado em 04.12.2019. Inteiro teor disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755364496

pelo Ministério Público à Receita Federal. Segundo o relator, Ministro Sebastião Reis, nas poucas referências que foram feitas no RE 1.055.941 quanto à possibilidade de requisição direta, o STF teria se manifestado pela sua ilegalidade, pelo que concluiu o Ministro Sebastião Reis que "em um Estado de Direito, não é possível admitir que órgãos de investigação, em procedimentos informais e não urgentes, solicitem informações detalhadas sobre indivíduos ou empresas, informações essas constitucionalmente protegidas, salvo autorização judicial"[375].

Esse fato reforça a necessidade de que o contexto em que se discute a privacidade seja levado em conta de forma expressa, a fim de se garantir maior segurança jurídica na atuação dos entes encarregados à persecução penal. Isso é ainda mais importante em matéria penal, onde, como já afirmado, a todo momento estão sendo discutidos limites para restrições a direitos fundamentais e, por isso mesmo, toda atuação estatal deve se dar de modo formal e materialmente adequado, sob pena de nulidade.

Outro processo onde se discute tema extremamente relevante para a demarcação da privacidade em matéria penal na sociedade da informação é o Tema 977 da repercussão geral do STF (que tem como recurso representativo de controvérsia o ARE 1042075), no qual se discute se, à luz do art. 5º, incs. XII e LVI, da Constituição da República, é lícita a prova produzida durante o inquérito policial decorrente do acesso, sem autorização judicial, de registros e informações contidas em aparelho de telefonia celular relacionado à conduta delitiva, hábeis a identificar o agente do crime. Em novembro de 2020, o relator, Min. Dias Toffoli, votou pela licitude, propondo a fixação da seguinte tese[376]:

> É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, **não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII).**

Cabe ressaltar que na decisão que afetou o recurso para julgamento sob o rito da repercussão geral, o Ministro Dias Toffoli já havia se manifestado no sentido de que no caso estava posta a colisão entre a inviolabilidade do sigilo das comunicações telefônicas, por um

---

[375] BRASIL. STJ. **A partir de precedente do STF, Terceira Seção considera ilegal obtenção direta de dados fiscais por iniciativa do MP.** Notícias STJ. 11.02.2022. Disponível em https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11022022-A-partir-de-precedente-do-STF--Terceira-Secao-considera-ilegal-obtencao-direta-de-dados-fiscais-por-iniciativa-do-.aspx

[376] BRASIL. SUPREMO TRIBUNAL FEDERAL. **ARE 1042075.** Extrato de sessão**.** Disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898

lado, e a impossibilidade de utilização, no processo, de provas supostamente obtidas por meio ilícitos, por outro. Trata-se, portanto, de um conflito normativo envolvendo a privacidade e a segurança pública, no qual se discute se a proteção à privacidade pode legitimar a restrição à descoberta da verdade para fins penais. Neste sentido, o relator ressaltou essa colisão afirmando que

> Essas garantias constitucionais mantêm estreito vínculo entre si e regulam e limitam a obtenção, a produção e a valoração das provas destinadas ao Estado, o que, no caso em apreço, será decisivo para se determinar a legitimidade da atuação da autoridade policial no papel de proceder à coleta de elementos e informações hábeis a viabilizar a persecução penal.
>
> Instaura-se, por isso, a discussão acerca do conteúdo e dos limites da proteção conferida pelo art. 5º, inc. XII, da CF, bem como da aferição da licitude da prova produzida durante o inquérito policial, dado que supostamente teria sido quebrado o sigilo das informações acostadas no aparelho celular do recorrido sem a pertinente autorização judicial.

Na sessão de 11 de novembro de 2020, após o voto do relator dando provimento ao recurso (que fora interposto pelo Ministério Público contra decisão que julgara ilícita a prova decorrente da análise do conteúdo de aparelho celular que o réu havia deixado cair na cena do crime), os Ministros Gilmar Mendes e Edson Fachin divergiram, propondo que tal acesso seja condicionado à "prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX)", estando o julgamento atualmente aguardando voto vista do Min. Alexandre de Moares[377].

É interessante notar que, em seu voto, o Ministro Dias Toffoli aparentemente se vale de uma visão de privacidade ligada à intimidade, provavelmente como decorrência do controle de constitucionalidade nesse caso ter como parâmetro a proteção constitucional ao sigilo das comunicações, previsto no inciso XII do art. 5º da CF/1988. Assim, o Ministro identificou como valores contrapostos a intimidade *versus* "os meios investigativos legais e a necessidade de ação rápida e efetiva para solucionar o fato, em especial a identificação dos autores do fato", tendo concluído que, por se tratar de uma situação de flagrância, não estaria caracterizada violação dos direitos fundamentais do réu, dado que "além de não ter havido violação do sigilo da comunicação de dados, o acesso a registro telefônico não acarretou risco

[377] BRASIL. SUPREMO TRIBUNAL FEDERAL. ARE 1042075. Rel. Min. Dias Toffoli. Disponível em https://portal.stf.jus.br/processos/downloadTexto.asp?id=5218109&ext=RTF

à intimidade do acusado nem ofensa à privacidade, mormente por não resultar em acesso a dados íntimos".

Esta avaliação remete à distinção entre dados de comunicação constitucionalmente protegidos e dados cadastrais, e se ancora muito fortemente na concepção de que a proteção constitucional ao sigilo reflete a proteção da intimidade, de modo que somente nos casos de acesso a informações sensíveis e sigilosas haveria propriamente violação à intimidade. Aliás, o relator, Min. Dias Toffoli, ressaltou o fato de que o tribunal de origem, ao proferir o acórdão recorrido, em nenhum momento tratou da questão da privacidade, mas apenas discutiu, no caso concreto, a extensão do sigilo das comunicações. Neste sentido, afirmou que

> Sem embargo de maior reflexão acerca da proteção constitucional dos direitos e garantias individuais em face da evolução dos aparelhos telefônicos móveis e do poder do Estado em tema de persecução penal, neste julgamento, limito-me a analisar o caso concreto e a acompanhar a jurisprudência já consolidada na Corte no sentido da licitude da prova produzida pela autoridade policial, sem autorização judicial, mediante o acesso à agenda e aos registros telefônicos d e aparelho celular apreendido no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações ou à privacidade do acusado (CF, art. 5º, inc. X e XII)[378].

Por outro lado, no voto divergente[379], o Ministro Gilmar Mendes sustenta que a distinção entre dados de comunicação protegidos e dados cadastrais merece ser revisitada, dado que as modernas tecnologias de informação e comunicação ensejaram modificação das circunstâncias fáticas e jurídica já que "cada vez mais, a nossa vida quase inteira está registrada em nossos aparelhos celulares.", por isso que os dados contidos nos celulares encontram-se " abrangidos pela proteção à intimidade e privacidade, constante do inciso X do mesmo art. 5º". Em seu voto, o Ministro parece adotar uma compreensão de privacidade mais próxima da autonomia informacional, chegando mesmo a citar lição de José Adércio Sampaio Leite reestruturando o direito à intimidade, dando-lhe conformação mais próxima à adotada neste trabalho:

> Em geral, define-se o direito à intimidade como uma espécie de editoria das informações pessoais ou como um genérico 'direito a ser deixado em paz'. Ele é mais do que isso e mais bem se apresenta como um direito à liberdade, marcado por um conteúdo mais determinado ou determinável, conjugado a um complexo de princípios constitucionais, que nada mais são do que suas manifestações concretas. [...] **Afirmar que o ser humano é livre exige, não como seu pressuposto, mas como consectário, reconhecer seu domínio ou**

[378] BRASIL. SUPREMO TRIBUNAL FEDERAL. ARE 1042075. Rel. Min. Dias Toffoli. Inteiro teor disponível em https://www.migalhas.com.br/arquivos/2020/11/ebc972578533af_4477905.pdf

[379] Disponível em https://www.migalhas.com.br/arquivos/2020/11/40d23b1087fc0f_4768547.pdf

> **controle sobre os inputs e outputs de informação**. Esse sentido natural da liberdade de traduz, no mundo jurídico, na liberdade 'informacional' próxima ao que o Tribunal Constitucional Federal alemão chamou de Informationelle Selbsstbestimmung, ou autodeterminação em matéria de informação, que conjuga o aspecto negativo de não impedimento ao positivo, de controle" (In: CANOTILHO, J. J. Gomes; MENDES, Gilmar; SARLET, Ingo; STRECK, Lênio Luiz. Comentários à Constituição do Brasil, p. 292-293)

Esse julgamento, ainda não concluído, poderá ajudar a firmar os contornos da proteção à privacidade em matéria penal, tendo presente a realidade digital em que estamos imersos, definindo qual o limite da atuação legítima do Estado e qual o nível adequado de proteção a ser conferido à intimidade e à privacidade do investigado. Verifica-se também a existência de compreensões diversas de privacidade entre os votos divergentes, o que deixa claro que, para possibilitar uma harmonização entre os valores colidentes, se adote uma concepção de privacidade que não se restrinja à intimidade ou ao controle de dados pessoais, mas antes, leve em consideração os contextos em que se insere a discussão da proteção da privacidade e a busca pela produção de provas penais.

Talvez um ponto de virada na abordagem dessa colisão entre a proteção da privacidade e os interesses de investigação e repressão de infrações penais possa emergir do debate acerca da criptografia ponta a ponta utilizada por aplicativos de comunicação instantânea. Como a tecnologia de processamento tornou-se barata e bastante disponível, qualquer pessoa com um *smartphone* simples pode se beneficiar da criptografia forte, gerando uma intensa discussão acerca da necessidade de se regular a criptografia, como a que se deu nos Estados Unidos no caso Apple San Bernadino[380] e, no Brasil, na discussão sobre o bloqueio judicial do WhastApp por não cumprir ordens judiciais de apresentação do conteúdo compartilhado entre usuários.

O tema está sendo decidido pelo Supremo Tribunal Federal na ADPF 403, de relatoria do Ministro Edson Fachin, que trata da suspensão dos serviços do aplicativo de comunicação por mensagem, por descumprimento de ordem judicial de apresentar o conteúdo de mensagens para instruir processo criminal, e na Ação Direta de Inconstitucionalidade (ADI) 5527, sob relatoria da Ministra Rosa Weber, na qual é questionada a interpretação de dispositivos do Marco Civil da Internet (artigos 10, parágrafo 2º, e 12, incisos III e IV, da Lei 12.965/2014), que têm servido de fundamentação para decisões judiciais que determinam a

[380] CF. RICHARDS, Neil. M. **The iPhone case and the future of civil liberties.** Boston Review, February 25, 2016. Disponível em https://www.bostonreview.net/us/neil-richards-apple-iphone-privacy.

suspensão dos serviços de troca de mensagens entre usuários da internet. Apesar de ainda não haver decisão final, nos votos proferidos pelos relatores se percebe uma nítida preocupação com a necessidade de se atualizar a compreensão da privacidade na era digital, adotando-se uma concepção contextual da privacidade. Como afirma a Ministra Rosa Weber, em seu voto,

> As expectativas razoáveis dos titulares dos direitos constitucionais devem ser mantidas. Qual é o sentido de uma Constituição que, no ano de 2020, protege o sigilo das comunicações telegráficas, mas não protege o sigilo das comunicações realizadas por aplicações de internet ou qualquer outro meio pelo qual as pessoas de fato se comunicam hoje? A Constituição não é um simulacro, não pode ser lida como se fosse um museu de direitos.[381]

Na mesma linha, o Ministro Edson Fachin buscou estabelecer algumas balizas que permitiriam efetuar uma adequada ponderação entre segurança e privacidade, afirmando que a demanda pela criptografia decorre da proteção que se espera ter da liberdade de expressão em uma sociedade democrática e que a criptografia protege os direitos dos usuários da internet, garantindo a privacidade de suas comunicações, sendo do interesse do Estado brasileiro encorajar as empresas e as pessoas a utilizarem a criptografia e manter o ambiente digital com a maior segurança possível. No voto, ele ressaltou que o maior desafio à proteção da privacidade ocorre nas hipóteses em que há dificuldades técnicas para se obter elementos de prova na apuração de crimes que gravemente violam direitos fundamentais, como, por exemplo, os casos de pornografia infantil e de condutas antidemocráticas, como manifestações xenófobas, racistas e intolerantes, que ameaçam o Estado de Direito[382].

Essa necessidade, inclusive, foi expressamente reconhecida no voto da Ministra Rosa Weber na ADPF 403, em que se questiona a constitucionalidade de dispositivos do Marco Civil da Internet (artigos 10, parágrafo 2º, e 12, incisos III e IV) que têm servido de fundamentação para decisões judiciais que determinam a suspensão dos serviços de troca de mensagens entre usuários da Internet. Em seu voto, a Ministra assentou que

> [...] **os maiores desafios contemporâneos à proteção da privacidade nada têm a ver com a imposição de restrições à liberdade de manifestação, enquanto relacionados, isto sim, aos imperativos da segurança nacional e da eficiência do Estado, à proliferação de sistemas de vigilância e à emergência das mídias**

[381] BRASIL. Supremo Tribunal Federal, ADI n. 5.527, Voto Ministra Relatora Rosa Weber. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[382] BRASIL. SUPREMO TRIBUNAL FEDERAL. ADPF 403. Disponível em http://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adpf403mc.pdf.

> **sociais, juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados.**
> Nesse contexto, pertinente, ainda, a contribuição de Alan Westing à doutrina jurídica da privacidade no mundo contemporâneo, ao caracterizar a estrutura desse direito como controle sobre os usos da informação pessoal. Nesse sentido, a privacidade, afirma, "é a pretensão de indivíduos, grupos ou instituições de determinarem para si quando, como e em que extensão a informação sobre eles será comunicada a outros".
> Tal concepção do direito à privacidade está alinhada com o reconhecimento do seu papel social na própria preservação da personalidade e no desenvolvimento da autonomia individual. (Voto da Min. Relatora Rosa Weber na ADI 5527 - *grifamos*)

Em sentido similar, ao proferir seu voto na ADPF 403, julgada em conjunto com a ADI 5527, o Ministro Edson Fachin afastou qualquer interpretação do marco civil da internet que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet e estabeleceu sete premissas:

> Primeira: o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais.
> Segunda: os direitos que as pessoas têm offline devem também devem ser protegidos online. Direitos digitais são direitos fundamentais.
> Terceira: a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet
> Quarta: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública.
> Quinta: A liberdade de expressão tem primazia prima facie e constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito.
> Sexta: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública.
> Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas.

À exceção da quarta premissa, que reflete a concepção da privacidade como controle

e, portanto, está sujeita às ressalvas anteriormente feitas (seção 3.2), todas as demais premissas vão no mesmo sentido daquilo que vem sendo defendido ao longo deste trabalho. Reconhecer o impacto das novas tecnologias sobre a persecução penal e sobre a própria noção do estado democrático de direito e da forma como devem ser tutelados os direitos fundamentais, é uma necessidade urgente. Aliás, sobre o tema, vale transcrever excertos do voto do Ministro Gilmar Mendes na ADI 6387 em que trata da necessidade de se compreender a inovação jurídica como contra-face da inovação técnica, afirmando a permanente abertura da ordem constitucional à transformação tecnológica. Após lembrar que atualmente os cidadãos, em todos os aspectos de sua vida, se veem obrigados a utilizar as novas tecnologias, e que isso acarreta riscos que incluem a possibilidade de o Estado penetrar na esfera privada do indivíduo, afirma que

> O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. A elevada concentração de coleta, tratamento e análise de dados possibilita que governos e de empresas utilizem algoritmos e ferramentas de data analytics, que promovem classificações e esteriotipações discriminatórias de grupos sociais para a tomada de decisões estratégias para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham.
> [...]
> Todo esse contexto nos indica que decisões críticas para o Estado de Direito estão sendo cada vez mais substituídas por mecanismos automatizados. Em outras palavras, de forma bem direta: vivemos na era das escolhas de Sofia automatizadas. Independente do acerto ou desacerto dessas decisões automatizadas, é inequívoco que a proteção dos valores estruturante da nossa democracia constitucional requer que o Direito atribua elementos de transparência e controle que preservem o exercício da cidadania.
> É por isso que, para muito além do mero debate sobre o sigilo comunicacional, este Tribunal deve reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo[383].

[383] BRASIL. SUPREMO TRIBUNAL FEDERAL. **ADI 6387 MC-REF/DF.** Plenário. Inteiro teor do Acórdão, p. 10-12. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629

5 CONCLUSÃO: A REGULAÇÃO DA INTERNET COMO INSTRUMENTO DA TUTELA DA PRIVACIDADE EM MATÈRIA PENAL

> Teorias são redes lançadas para capturar o que chamamos de "o mundo": para racionalizá-lo, explicá-lo e domá-lo. Queremos fazer as malhas cada vez mais e mais finas (Popper, 1959, p. 59)

A compreensão das profundas alterações por que passa a sociedade contemporânea em razão da imersão cada vez maior da população no mundo digital deixa evidente a necessidade de que a proteção dos direitos fundamentais do indivíduo seja feitas a partir de uma compreensão mais ampla e complexa dos limites da atuação estatal na esfera penal. De fato, as visões tradicionais de privacidade, que a reduzem à sua dimensão individual, não se mostram suficientes para possibilitar a construção de uma esfera de proteção individual em um mundo no qual a informação se tornou componente fundamental da produção econômica e é compartilhada e processada a todo instante e com a concordância, expressa ou tácita, dos titulares de dados.

A tecnologia deve ser compreendida a partir de suas consequências concretas nas relações sociais, sem que se perca de vista o fato de que ela é um produto das relações sociais, sendo construída a partir de determinados interesses e com vistas a alcançar determinados objetivos que muitas vezes têm pouca relação com as maravilhas prometidas por seus defensores. Por isso que a análise das relações entre tecnologia e sociedade não podem ser feitas acriticamente, dado que, apesar das belíssimas promessas que as novas tecnologias da informação e comunicação apresentam, sua regulação e o tratamento que o direito dá a elas deve se pautar por dados concretos decorrentes de sua aplicação, e não a partir de suas possibilidades.

A partir da ação dessa postura é que se torna possível evitar o risco de, ao se ponderar a utilização das novas tecnolgias (v.g. big data, inteligência artificial, metaverso, reconhecimento biométrico, etc) com a segurança pública, a ordem social ou qualquer outro interesse coletivo, cair em abstrações que apenas servem para reduzir a proteção do indvíduo contra a atuação dos poderes econômicos e políticos.

Por isso, o tratamento que o direito, e em especial o direito processual penal, confere à privacidade no mundo digital ocupa um lugar de suma importância para o Estado de Direito. As informações fornecidas pelos usuários estão em todo lugar e os limites para a sua

utilização secudária frequentemente não são muito claros, especialmente em matéria penal. Veja-se que aqui estamos pensando em informações em seu sentido mais largo, que incluem, entre outros aspectos, as postagens em redes sociais, as pesquisas realizadas em motores de busca, os dados de georeferenciamento fornecidos pelos GPSs dos celulares, dados biométricos compartilhados com sites do governo ou de empresas privadas, etc. Em suma, as informações compartilhadas pela internet e que facilitam enormemente a vida dos indivíduos, podem criar um ambiente de absoluta vigilância digital que, no limite, pode reduzir a letra morta os limites tradicionalmente estabelecidos á atividade persecutória do Estado e à própria existência de um espaço de liberdade individual. Num estado de vigilância total, elementos que configuram verdadeiros pilares do estado democrático de direito estão em constante tensão e o risco não é apenas o de uma reduçlão geral da liberdade em razão da vigilância, mas também há um aumento exponencial no risco de mau uso das informações. Basta se pensar na possibilidade da utilização indevida das informações pessoais sigilosas como instrumento de perseguições políticas ou religiosas, por exemplo.

Nesse ponto, vale ressaltar que a existência de um círculo íntimo de informações sensíveis e protegidas do acesso por terceiros é elemento essencial da integridade da personalidade humana, cujo desenvolvimento pressupõe a possibilidade de manutenção de determinados aspectos ocultados de outras pessoas ou grupos. Todos nós precisamos desse espaço de proteção. Com efeito, não se pode aqui cair na provocação dos que, para defenderem a vigilância, sustentam que "quem não deve não teme". Na verdade, todos somos um amálgama de vários papéis desempenhados em diferentes contextos sociais e frequentemente há diferenças substanciais entre os papeis desempenhados em cada contexto.

Na realidade, o convívio social impõe mesmo a necessidade de que determinados aspectos de nossa personalidade e posicionamentos sejam ocultados. Basta pensar em como seriam nossas relações no trabalho, na igreja ou mesmo na família se todos os nossos pensamentos acerca dos demais integrantes daquele grupo social fossem tornados públicos. Além disso, o papel desempenhado em um determinado grupo social, em um determinado contexto, por vezes é bem diferente do papel desempenhado em ouros contextos. Um estudante gay que seja ativista pela diversidade no contexto escolar, por exemplo, pode optar por manter sua sexualidade ocultada no contexto familiar ou profissional. Enfim, as pessoas desempenham papéis diferentes e têm direito de manter determinados aspectos de suas vidas ocultados do escrutínio de outras pessoas e grupos e o acesso indevido a essas informações pode fragilizar o titular desses dados, abrindo margem para o mau uso intencional ou não dessas informações. A privacidade, portanto, nos protege a todos, já que, sem exceção, todos

temos aspectos que queremos ver escondidos e isso não só é natural como é absolutamente necessário para o convívio social.

Some-se a isso o fato de que, na maior parte das vezes, as informações compartilhadas por meio da internet em razão da utilização de aplicativos conectados à rede, são fornecidas para finalidades absolutamente singelas e corriqueiras, ou até mesmo ligadas ao exercício de direitos da cidadania, como ocorre no caso do cadastramento na plataforma digital do Poder Executivo (Gov.br), que exige, para conferir o status de conta "ouro", o fornecimento de dados biométricos do usuário. Recentemente esse cadastramento foi exigido para que os interessados pudessem acessar as informações acerca da existência de saldos de depósitos bancários "esquecidos" em contas correntes inativas, de modo que todos que quisessem reaver esses eventuais valores deveriam ter que cadastrar seus dados biométricos na plataforma.

Tal utilização, assim como as demais decorrentes da plataforma governamental, nada tem com a persecução penal. Entretanto, não há dúvida de que a habilitação do indivíduo para utilizar esse serviço gera um imenso banco de dados que poderá no futuro vir a ser integrado a sitemas de reconhecimento facial e às câmeras de vigilância, possibilitando a localização de pessoas de interesse para a jurisdição penal em tempo real. Isso só para ficar em um dos exemplos que mais vem sendo discutidos na atualidade, diante dos notórios casos de erros e vieses na identificação facial. A extraordinária multimplicação do fenômeno da datificação e as facilidades decorrentes do barateamento das tecnologias, conjugado ao gigantesco salto na capacidade de processamento dos modernos sistemas de *Big data* e inteligência artifical, fazem com que as possibilidades de utilização dos dados compartilhados pela rede mundial de computadores não tenham limites.

Essa perceção do valor da privacidade para o indivíduo e para a coletividade deve ser conjugada à superação da visão tecnodeterminista e à compreensão de que a tecnologia não é, por si, a resposta para todos os problemas sociais, já que os algoritmos refletem os vieses existentes na sociedade, podendo muitas vezes contrubuir não só para a manutuenção, mas até mesmo para o agravamento de distorções e desigualdades, especialmente no campo penal que, pela sua própria natureza, já ostenta esse caráter de seletividade na proteção de bens jurídicos e na proibiçlao de condutas de determinados crupos sociais.

É muito tentadora a ideia de que o uso da tecnologia irá criar as condições necessárias para que o sistema penal seja mais eficiente, protegendo as pessoas contra a criminalidade. Entretanto, adotar-se esse discurso de forma acrítica é simplesmente fechar os olhos para o caráter social da construção das tecnologias e deixar de perceber que o mundo digital é construído a partir de algoritimos programados para operar de acordo com formas pré-

determinadas. A inteligência artificial não se cosntitui a partir do nada, mas sim a partir de correlações feitas a partir de uma base de dados gigantesca e repleta de vieses, que em grande medida reproduzem a visão de mundo de seus criadores.

Por tudo isso, é preciso que as novas tecnologias sejam pensadas e reguladas pelo direito a partir de uma noção fundada na ideia da necessidade de tutela de direitos fundamentais. Não se pode compreender a atividade regulatória como mero instrumento de controle de atividades econômicas tendente a combater falhas de mercado. O escopo deve ser mais amplo, incluindo a tutela dos direitos fundamentais dos indivíduos como elemento essencial da atuividade regulatória. E, para isso, a é necessária uma nova compreensão da privacidade, que não mais se limite às visões que a reduzem às dimensões da intimidade ou do controle de dados pessoais. Ainda que essas dimensões sejam importantes – e obviamente não se pretende de forma alguma negar essa importância – elas são insuficientes para garantir aos indivíduos proteção efetiva contra a possibilidade de utilização secundária dos dados compartilhados, de modo que se faz necessária a adoção de uma teoria que permita compreender a privacidade de acordo com o contexto em que a informação é produzida.

Com efeito, sem a adoção de uma teoria multidimensional da privacidade, que inclua as noções de integridade contextual, a privacidade passa a ser entendida como fenômeno meramente individualista, que, quando da podenração, quase sempre irá ceder ante os interesses coletivos que a ela são contrapostos. De fato, sem a compreensão do caráter coletivo e social da privacidade, bem como de sua importância isntrumental para a liberdade, a igualdade e a democracia, ela quase sempre será vista como um mero incômodo aos relevantes interesses do combate à criminalidade ou à manutenção da ordem pública.

Por isso é que a adoção de teorias e concepções incompletas da privacidade tendem a gerar soluções que não se apresentam adequadas a efetivamente servir de elemento de pacificação social, garantindo estabilidade e segurança jurídica. Questões ligadas ao limite da privacidade na era digital e suas repercussões na seara penal, assim, cada vez mais assumem papel de absoluto relevo na sociedade contemporânea, de forma que talvez seja necessário fazer uma "ortopedia" de alguns institutos jurídicos, adaptando-os à nova realidade, para que eles sigam tendo capacidade de rendimento.

O Direito Penal, entendido como mais poderoso instrumento de tutela de direitos fundamentais de que dispõe o Estado, é fortemente impactado por toda essa mudança, por isso que é necessário se estabelecer um arcabouço teórico que permita conjugar a tutela dos direitos fundamentais com a eficiência e efetividade dos instrumentos de persecução penal, de

forma adequada à realidade atual, o que pressupõe compreender a privacidade em toda sua multidimensionalidade.

As novas tecnologias criam inúmeras novas possibilidades no campo probatório, abrindo margem para, no limite, implementar-se um ambiente de vigilância total, no qual o indivíduo poderia ser tolhido de seu espaço de ser, pensar e agir de forma separada e independente. A privacidade, por isso, não pode ser compreendida unicamente sob uma dimensão individual, mas deve ser compreendida e valorada a partir da compreensão de sua dimensão coletiva, que está relacionada não só à liberdade e à igualdade, mas à própria democracia.

É preciso, pois, vencer a tentação de aproveitar das facilidades que as modernas tecnologias de informação e comunicação propiciam para, numa abordagem eminentemente utilitarista, obter maior eficiência no controle e vigilância, ainda que a um custo extremamente elevado em termos de dignidade da pessoa humana. A persecução penal deve encontrar limites epistemológicos na proteção da privacidade, que não é um direito absoluto, mas é um direito qualificado, cuja relativização e restrição pressupõe uma apreciação concreta de todas as condições fáticas e jurídicas envolvidas na colisão normativa.

Nesse sentido, resta claro que um modelo teleológico de direito penal não pode ser definido em termos consequencialistas ou puramente pragmáticos, tendo unicamente como norte a busca pela prevenção eficaz do delito (critérios de uma Política criminal *empírica*), mas deve buscar uma política criminal *valorativa*, onde as as razões de política criminal possam se integrar à dogmática jurídica como forma de limitar o *ius puniendi* estatal, aumentando as esferas de proteção do cidadão, ao mesmo tempo em que garantem as bases para uma proteção mais eficaz dos bens jurídicos tutelados[384].

Por isso é importante reforçar a ideia de que o direito penal deve ser entendido como instrumento de tutela de direitos fundamentais, voltado sempre à proteção de bens jurídicos de extração constitucional. Essa perspectiva é que permite compreender que a política criminal deve ter sempre como objetivo final a tutela de tutela dos direitos fundamentais e da dignidade do ser humano, inclusive daqueles que eventualmente ocupem a posição de investigado, réu ou condenado. Em um estado democrático de direito, portanto, não há espaço para a defesa de uma visão do direito penal e da política criminal unicamente voltada à eficiência da "segurança pública".

---

[384] SILVA SANCHEZ, Jesus-Maria . **Política criminal en la dogmática: algunas cuestiones sobre su Contenido y límites.** *In* SÁNCHEZ, Jesus-Maria Silva. (org.) **Política criminal y nuevo sistema penal. Libro homenage a Claus Roxin.** Barcelona: José Maria Boschi editor, 1997**.** P. 22-23

Na realidade, uma vez adotada essa ótica, fica evidente que sequer deveria haver espaço para se pensar numa dicotomia entre segurança pública e direitos fundamentais do indivíduo, posto que, na verdade, tratam-se de conceitos complementares, que só existem verdadeiramente quando coexistem. Não há efetiva segurança cidadã sem respeito aos direitos fundamentais, da mesma forma que é inimaginável a tutela de direitos fundamentais sem que o Estado disponha de um instrumental que lhe possibilite impor à população, por meio da coerção, o respeito a bens jurídicos.

Nesse ponto, chega-se à uma interessante confluência entre o processo penal e a teoria regulatória aqui adotada, que empresta à atividade regulatória uma finalidade mais ampla do que a mera correção de falhas do mercado, para também incluir objetivos ligados à tutela do interesse público, mais especificamente àqueles valores constitucionalmente previstos como direitos fundamentais.

Ora, se a regulação da privacidade digital deve ter como norte a tutela de direitos fundamentais, se a tutela da intimidade, da vida privada e da proteção de dados, inclusive nos meios digitais, são direitos fundamentais expressos na Constituição, e se o processo penal deve reconhecer como limites extrínsecos à atividade probatória o respeito a tais direitos fundamentais, segue-se que a regulação da internet e das novas tecnologias de informação e comunicação devem ser entendidas também como instrumentos de tutela de direitos fundamentais em matéria penal.

Por isso também é importante a compreensão da relação entre a sociedade e a tecnologia, aportando elementos que permitam superar a visão tecnodeterminista que desconecta a tecnologia da sociedade e a recebe como algo isento de viés. Especialmente quando se compreende que a utilização cada vez mais ampla e profunda das novas tecnologias no campo da persecução penal encerra riscos, inclusive o de reproduzir nos algoritmos os vieses próprios do sistema penal, é preciso se manter vigilante para perceber que o papel de escudo de proteção dos direitos fundamentais exercido pelo direito penal deve ser complementado por uma atividade regulatória das novas tecnologias também voltada a essa finalidade.

A regulação da privacidade nos meios digitais, assim, ao estipular os limites de coleta, compartilhamento, processamento e utilização dos dados na internet assume a condição de limite epistemológico à produção de prova em matéria penal, sendo certo que essa limitação deverá ser compreendida em dois aspectos: o primeiro, ligado à atividade regulatória propriamente dita, quando o legislador ou o regulador (agência reguladoras ou outras autoridades administrativas com competência para editar normas regulamentadoras) deverão

ter em mente a necessidade de estabelecer, em abstrato, as possibilidades de coleta de dados, bem como seu compartilhamento, análise, armazenamento e utilização.

Nesse aspecto, tem-se que a atividade regulatória pode se dar tanto pela instituição de uma proibição, como por exemplo o impedimento da coleta de dados que não sejam necessários à finalidade para a qual se destinam, mas também pode se dar pela regulamentação da utilização secundária dos dados. Retomando o exemplo do cadastro biométrico feito para a plataforma de serviços digitais do Poder Executivo (Gov.Br), tem-se que, nesse caso, uma eventual regulação poderia se dar pela proibição da coleta de determinados dados que não sejam especifica e diretamente relacionados ao serviço oferecido (poderia haver proibição da coleta de informações relacionadas à orientação sexual ou credo religioso, por exemplo). Por outro lado, a restrição regulatória também poderia se dar através da restrição ao compartilhamento e utilização secundária dos dados para algumas finalidades específicas. Assim, o regulador poderia, por exemplo, limitar a utilização, o compartilhamento e o processamento dos dados biométricos para os casos de investigação de crimes graves (vg. punidos com reclusão), tal como ocorre em relação à interceptação telefônica, por exemplo, na qual o art. 2º, III da Lei 9.296/96 impede a utilização da intercepetação telefônica para investigação de crimes punidos com detenção.

O outro aspecto em que a regulação da privacidade digital funciona como limite epistemológico à produção de provas em matéria penal é aquele especificamente relacionado à produção probatória em casos concretos, em investigações e ações penais em curso, hipótese em que o limite epistemológico tem em mira a atuação do juiz na condução do processo. Nesses casos, caberá ao juiz, ao analisar a validade da atividade instrutória, realizar a operação mental de ponderação concreta dos valores colidentes (v.g. necessidade de produção probatória para garantir a aplicação da lei penal *versus* proteção da intimidade).

Importante notar que, nesse caso, o âmbito de atuação estatal válida constitui um dado prévio, decorrente da limitação previamente realizada pelo regulador ao estabelecer os limites epistemológicos que conformam a atuação do julgador. Por isso, ao se admitir a ponderação de valores para a solução da situação concreta, não se cuida aqui de romper a barreira deontológica de proteção criada pela noção de direitos fundamentais do indivíduo, mas unicamente de estabelecer, dentro dos limites já previamente estabelecidos pelo legislador, quais as provas legal e moralmente admissíveis em um determindo contexto de colisão de valores (notadamente segurança pública e intimidade), posto que, como já afirmado, toda atividade persecutória representa uma incursão sobre a esfera de privacidade do investigado/réu.

Assim, quando se tem em mente as limitações probatórias que se impõem à atuação do aplicador do direito a casos concretos, não se cogita propriamente de uma colisão entre princípios e regras, posto que, a rigor, trata-se de reconhecer que determinados princípios foram validamente restringidos pelo legislador por meio de regras, valendo notar que a legalidade estrita é um princípio formal basilar do sistema jurídico, por isso que tanto mais efetiva será a restrição feita pelo legislador quanto mais forte for o respeito a tais princípios formais. Em todo caso, para a compreensão da privacidade digital como limite epistmológico à produção probatória em matéria penal, é suficiente ressaltar que, na aplicação concreta do direito em matéria de persecução penal, a regulação da privacidade feita pelo legislador e em alguns casos pelo regulador (por exemplo, através de regulamentos de agências reguladoras, como Anatel, Cade, ANPD) representam limites à atividade probatória que, no mínimo, impõem um grande ônus argumentativo ao aplicador que queira superá-los.

De toda sorte, em ambos os aspectos da limitação da produção probatória em mateéria penal, isto é, tanto na atuação regulatória abstrata quanto na aplicação do direito aos caos concretos, para que a ponderação entre a necessidade de garantia da ordem e segurança pública em face da proteção da privacidade não seja uma escolha arbitrária e voluntarista, é necessária a existência de uma teoria de base que permita a criação de regras de validade para a utilização de informações compartilhadas pela internet.

Nesse sentido, sustentamos a necessidade de que a regulação da privacidade no mundo digital seja feita a partir de uma abordagem multidimensional e contextual que, sem, abrir mão dos importantes aspectos individuais da proteção da privacidade, relacionados à proteção da intimidade e ao controle dos dados compartilhados (autonomia informacional), também permita incorporar à privacidade o peso de sua dimensão coletiva. Para isso, a privacidade deve ser compreendida a partir de uma concepção de integridade contextual, que permite identificar violações à privacidade a partir das noções de normas sociais que regem determinados contextos de fluxo de informações.

As pessoas produzem dados e compartilham informações a partir de determinados contextos e visando a determinadas finalidades. A utilização de dados produzidos em um contexto para finalidades diversas, configura necessariamente uma lesão à privacidade que somente pode ser justificada à vista de elementos concretos que apontem não só a imprescindiblidade da medida como a inexistência de alternativas menos gravosas de obtenção da informação. Por isso, a atuação tanto do regulaor (incluindo-se aqui o legislador) quanto do julgador devem estar atentos ao peso e precedêcnia da privacidade em uma sociedade democrática.

Critérios auxiliares de avaliação da legitimidade da vulneração da privacidade devem respeitar as normas sociais relativas ao fluxo de informações compartilhadas pela internet. O indivíduo que faz o cadastro biométrico no Gov.br, por exemplo, tem a legítima expectativa de que essa informação sensível seja mantida em sigilo e que sua foto não acabe alimentando um banco de dados de identificação criminal a ser utlizada em delegacias de polícia. As expectativas sociais acerca da proteção dos dados compartilhados constituem os elementos básicos que formam o substrato da integridade contextual, noção que possibilita analisar se determinada violação da privacidde pode ser considerada legítima ou não.

Nesse aspecto, uma abordagem da privacidade fundada na integridade contextual deve partir da análise de regras de duas categorias: as relacionadas à pertinência e as relacionadas às normas de distribuição das informações.

A pertinência diz respeito à quais informações podem ser reveladas em um dado contexto. No contexto de um atendimento médico em uma emergência ou pronto socorro, por exemplo, é apropriado que informações acerca do estado de saúde anterior do paciente sejam revelados. Da mesma forma, a discussão sobre a situação financeira de m indivíduo é adequado quando ele procura um agente financeiro para obtenção de um empréstimo. A pertinência, portanto, tem ligação com existência de uma relação de adequação entre a informação e o contexto em que ela será utilizada.

Por outro lado, as normas de distribuição têm ligação com a possibilidade de que a transmissão de determinadas informações, que em seus contextos originais tenham atendido às regras de pertinência, mantenham essa pertinência ante diferentes contextos para os quais sejam enviadas. Nos exemplos utilizados acima, por exemplo, tem-se que por mais que as informações relativas à saúde do paciente tenham sido produzidas de modo adequado no contexto de um atendimento médico, em uma entrevista de emprego, muito dificilmente a revelação de tais dados poderá ser tida como apropriada. Esa tarnsmissão, portanto, seria indevida e violaria a privacidade do indivíduo. Da mesma forma, a divulgção das informações financeiras seria completamente apropriadas na discussão com a instituição financeira, mas não no ambiente de trabalho dessa pessoa. A discussão aqui diz respeito aos limites à utilização secundária dos dados e guarda relação com as expectativas sociais geradas a partir da finalidade para a qual os dados foram fornecidos.

Qualquer violação à pertinência dos dados ou às sua expectativa de distribuição configura uma violação à integridade contextual. Identificar essas características no imenso fluxo de informações disseminadas no nosso mundo cada vez mais imerso no digital torna

possível analisar de forma menos voluntariosa e mais adequada à tutela dos direitos fundamentais dos indivíduos se uma dada utilização é legítima ou não.

A identificação de possíveis violações à privacidade a partir desses critérios de pertinência e distribuição permite que a ponderação e o balanceamento a serem feitos na regulação ou na aplicação concreta do direito garanta a um só tempo a necessária proteção à privacidade, dado que as violações serão mais facilmente identificáveis como tal e ao mesmo tempo cria condições para que, em determinados casos, se admita que informações produzidas em um dado contexto possam ser utilizadas em outro contexto, para finalidades de persecução penal, quando houver razões suficientes para que a balança penda a favor da segurança.

Em todo caso, a adoção de uma teoria regulatória fundada no interesse público, aliada à uma concepção multidimensional da privacidade, ligada à integridade contextual, cria as bases para que se busque o equilíbrio entre segurança e privacidade no mundo digital, superando-se algumas dicotomias que tradicionalmente embotam os debates nessa matéria, como por exemplo a distinção entre público/privado, ou entre informações pessoais sensíveis e meras informações ou, ainda, entre dados coletados pelo poder púbico e dados coletados por entes privados.

A privacidade, quando entendida em toda sua complexidade, ocupa um lugar central na construção do contrato social e sua proteção adequada configura medida essencial para a efetiva construção do estado democrático de direito. Ao buscar elementos que permitam estabelecer critérios a serem analisados para a validação das restrições à produção de provas em matéria penal, o que se busca é estabelecer os limites e possibilidades para a utilização de dados disseminados pela internet de forma a garatir que as novas tecnologias de informação e comunicação sejam eficazmente utilizadas sem se constituírem em um risco excessivo à liberdade e à democracia.

REFERÊNCIAS

ABBATE, Janet. **Inventing the internet.** Cambridge: The MIT Press, 2000.

ADEODATO, João Maurício. **Ética e retórica: para uma teoria da dogmática jurídica.** 4. ed. São Paulo: Saraiva, 2009, p. 151

ALEXY, Robert**. El concepto y la validez del Derecho**. 2. ed. Barcelona: Gedisa, 1997.

_____, **Teoria da argumentação jurídica**, São Paulo: Landy, 2001.

_____. **Direitos fundamentais, balanceamento e racionalidade**. Ratio Juris. Vol. 16, n. 2, junho de 2003.

_____. **Teoria dos direitos fundamentais.** São Paulo: Malheiros, 2008.

_____. **Direitos fundamentais, balanceamento e racionalidade**. Ratio Juris. Vol. 16, n. 2, junho de 2003.

ALMEIDA. José Raul Gaviã o. **Anotações acerca do direito à privacidade**. *in* MIRANDA, Jorge e SILVA, Marco Antonio Marques (cord). **Tratado luso-brasileiro da dignidade humana.** 2a. edição. São Paulo: Quartier Latin, 2009

ANDREWS, Lori. **I know who you are and I saw what you did, Social networks and the death of privacy.** 2012.

ANTUNES, Marco António. **O público e o privado em Hannah Arendt.** Biblioteca On Line de Ciências da Comunicação, 2004. **Disponível em http://www.bocc.ubi.pt/pag/antunes-marco-publico-privado.pdf**

ARENDT, Hannah. **A condição humana. 10ª. Ed.** Rio de Janeiro: Forense Universitária, 2007.

RODOTÀ, Stefano. **A vida na sociedade da vigilância. A sociedade hoje.** Rio de Janeiro: Renovar, 2008

ARISTÓTELES. **Ética a Nicômaco.** Tradução de Leonel Vallandro e Gerd Bornheim. Livro V, 6. 1134a 26-28**.** São Paulo: Nova Cultural, 1991.
ÁVILA, Humberto Bergmann, **A distinção entre princípios e regras**, Revista Diálogo jurídico, vol. I, nº 4. Disponível em << http://www.direitopublico.com.br/pdf_4/DIALOGO-JURIDICO-04-JULHO-2001-HUMBERTO-AVILA.pdf>> acesso em 10.06.2012 p. 14.

BADARÓ, Gustavo. **Editorial dossiê "Prova penal: fundamentos epistemológicos e jurídicos".** Revista Brasileira de Direito Processual Penal. Vol. 4, n. 1, 2018. disponível em https://revista.ibraspp.com.br/RBDPP/article/view/138/117

BAIN, Read. **Technology and State Government**. American Sociological Review, vol. 2, no. 6, 1937, pp. 860–874. disponível em www.jstor.org/stable/2084365.

BALDWIN, Robert, CAVE, Martin Cave e LODGE, Martin. **Introduction: Regulation—the Field and the Developing Agenda.** in BALDWIN, Robert, CAVE, Martin Cave e LODGE, Martin (orgs.). **The Oxford Handbook of Regulation.** Oxford: Oxford University Press, 2010

BALL, Kirsten *et al*. **A Report on the Surveillance Society For the Information Commissioner by the Surveillance Studies Network.** Disponível em https://www.personuvernd.is/media/frettir/surveillance_society_full_report_final.pdf

BANDEIRA DE MELLO ,Celso Antônio, **Curso de direito administrativo**, 14ª. ed. São Paulo: Malheiros, 2002. p. 408.

BAPTISTA ,Patrícia e KELLER, Clara Iglesias. **Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas.** RDA – Revista de Direito Administrativo, Rio de Janeiro, v. 273, p. 123-163, set./dez. 2016

BARBOSA-FOHRMANN. Ana P. **Algumas incursões sobre o significado de espaço público nos pensamentos de Hannah Arendt, Jürgen Habermas, Charles Taylor e Nelson Saldanha**. Diálogos Latinoamericanos n° 10. V. 1, 2005. PP. 73-97. Disponível em https://www.academia.edu/3323628

BARLOW, John Perry. **Uma declaração da independência do ciberespaço.** Tradução de MERLO, Rafael Augusto Arruda. Disponível em http://www.mediafire.com/file/2a9pdct2kaervdp/John+Perry+Barlow+-+1996+-+Uma+Declara%C3%A7%C3%A3o+da+Independ%C3%AAncia+do+Ciberespa%C3%A7o.pdf

BARROSO, Luiz Roberto. **Curso de direito constitucional contemporâneo.** Os conceitos fundamentais e a construção de um novo modelo. São Paulo: Saraiva, 2009.

BARROSO, Luís Roberto, **Interpretação e aplicação da constituição**, São Paulo: Saraiva. 2011

BASTOS, Celso.**Curso de Direito Constitucional**. São Paulo: Saraiva, 2001.

BAUDRILLARD, Jean. **À sombra das maiorias silenciosas O fim do social e o surgimento das massas.** São Paulo: Editora Brasiliense, 1985.

BENNETT, Colin e PARSONS. Christopher. **Privacy and surveillance: the multidisciplinary literature on the capture, use and disclosure of personal information in cyberspace**. In DUTTON, Willian H. The Oxford handbook of Internet studies. Oxford: Oxford University Press. 2014.

BECK, Ulrich. **Sociedade de risco. Rumo a uma outra modernidade**. Trad. Sebstião Nascimento. São Paulo: Editora 34, 2010.

_____. **A Política Na Sociedade de Risco.** Revista eletrônica Ideias – Unicamp - v. 1, n. 1, 2010. Disponível em http://www.ifch.unicamp.br/ojs/index.php/ideias/article/view/66/62

BERNERS-LEE, Tim. **Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor**, San Francisco: HarperCollins, 2000.

BIONI, Bruno Ricardo. **Proteção de dados pessoais. a função e os limites do consentimento**. 2a. edição. Rio de Janeiro: Forense, 2020

BIONI, Bruno e MARIA, Luciano. **O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o Seu Portal de Entrada?** Em FRAZÃO, ANA e MULHOLLAND, Caitlin. **Inteligência artificial e direito.** São Paulo: Revista dos Tribunais, 2020. Disponível em https://brunobioni.com.br/home/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf

BLACK, Julia. **Critical Reflections on Regulation**, LSE Centre for the Analysis of Risk and Regulation Discussion Paper 4, 2002. Disponível em http://www.lse.ac.uk/accounting/CARR/pdf/DPs/Disspaper4.pdf

BOBBIO, Norberto. **Teoria do ordenamento jurídico**, 10ª. ed. Brasília: ed. Unb. 1999. pp 158-159

BRASIL. SUPREMO TRIBUNAL FEDERAL. ADPF 403. Disponível em http://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adpf403mc.pdf.

BRASIL. SUPREMO TRIBUNAL FEDERAL. ARE 1042075. Rel. Min. Dias Toffoli. Disponível em https://portal.stf.jus.br/processos/downloadTexto.asp?id=5218109&ext=RTF

BRASIL. Supremo Tribunal Federal, ADI n. 5.527, Voto Ministra Relatora Rosa Weber. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

BRASIL. SUPREMO TRIBUNAL FEDERAL, ADPF 130. Rel. Min. Ayres Britto.

BRASIL. SUPREMO TRIBUNAL FEDERAL.RE n. 603.616/RO, Rel. Ministro Gilmar Mendes, DJe 8/10/2010.

BRASIL. SUPREMO TRIBUNAL FEDERAL. ADI 6387 MC-Ref. Tribunal Pleno. Rel. Min. Rosa Weber. Julgado em 07.05.2020. Disponível em https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false

BRASIL. SUPREMO TRIBUNAL FEDERAL. RE 1010606/RJ. Voto do Ministro Dias Toffoli, p. 39. J. em 11/02/2021. Disponível em https://jurisprudencia.stf.jus.br/pages/search/sjur446557/false

BLACK, Julia. **Critical Reflections on Regulation**, LSE Centre for the Analysis of Risk and Regulation Discussion Paper 4, 2002. Disponível em http://www.lse.ac.uk/accounting/CARR/pdf/DPs/Disspaper4.pdf.

BROWNSWORD, Roger; SCOTFORD, Eloise, e YEUNG, Karen. **Law, Regulation, and Technology: The Field, Frame, and Focal Questions.** In BROWNSWORD, Roger;

SCOTFORD, Eloise, e YEUNG, Karen (orgs). The Oxford Handbook of Law, Regulation and Technology.Oxford: Oxford University Press, 2017.

CANARIS, Claus-Wilhelm. **Direitos fundamentais e direitos privados.** Coimbra: Almedina, 2009.

CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro.** Sequência, n. 76, p. 225. Disponível em

CARBONELL, Miguel. **El principio de proporcionalidad y los derechos fundamentales**. in CARBONELL, Miguel (org.). El principio de proporcionalidad y la interpretación constitucional**.** Quito: Ministerio de Justicia y Derechos Humanos, 2008.

CARNEIRO, Luiz Orlando. Portal Jota. disponível em https://jota.info/justica/capital-estrangeiro-anj-pede-ao-stf-que-portais-de-noticias-na-internet-sejam-equiparados-jornais-impressos-20102016

CASTELLS, Manuel. **A Sociedade em Rede – a Era da Informação: economia, sociedade e cultura**. 14a Reimpressão. São Paulo: Paz e Terra, 2011 .

CASTELLS, Manuel. **O poder da comunicação.** São Paulo: Paz e Terra, 2015

CAVE, Stephen e ÓHÉIGEARTAIGH, Seán S. **An AI Race for Strategic Advantage: Rhetoric and Risks**, 2018. Disponível em http://www.aies-conference.com/wp-content/papers/main/AIES_2018_paper_163.pdf.

CHRISTOFOROU, Theofanis. **The precautionary principle, Risk Assessment, and the comparative role of Science in the european Community and the US legal system.** In FAURE, Michael G. e Norman J. VIG (ed)– Green Giants? Enviromental policies of the Uniteds States and the european . Cambridge: The MIT Press, 2004, pp. 17–51.

COHEN, Julia. **Surveillance versus privacy: effects and implications.** in GRAY, David, HENDERSON, Stephen E., (orgs). **The Cambridge handbook of surveillance law.** New York: Cambridge University Press, 2017.

CORBETT, Philip B. **It's Official: The 'Internet' Is Over**. The New York Times, Junho de 2016. Disponível em https://www.nytimes.com/2016/06/02/insider/now-it-is-official-the-internet-is-over.html

COX, Joseph. **Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies.** Motherboard, 2019. disponível em https://www.vice.com/en_us/article/zmpgmx/facebook-stops-graph-search

CROSS, Frank B. **When Environmental Regulations Kill: The Role of Health/Health Analysis**, Ecology Law Quartely, Nº 22, 1995. Disponível em: http://scholarship.law.berkeley.edu/elq/vol22/iss4/2. Acesso em 18/07/2015

_____. **Paradoxical Perils of the Precautionary Principle**, Washington & Lee Law Review. Nº 851, 1996. Disponível em http://scholarlycommons.law.wlu.edu/wlulr/vol53/iss3/2. Acesso em 18/07/2015.

DAHL, Robert. **Democracia e seus críticos.** São Paulo : Editora WMF Martins Fontes, 2012**.**

DANTAS, David Diniz. **Interpretação constitucional no pós-positivismo.** São Paulo: Madras, 2004.

DENARDIS, Laura. **The Global war for internet governance.** New Haven: Yale University Press, 2014.

DEVRIES, Will Thomas. **Protecting Privacy in the Digital Age**, 18 Berkeley Tech, 2003. Disponível em http://scholarship.law.berkeley.edu/btlj/vol18/iss1/19

DÍEZ RIPOLLÉS, José Luis. **El nuevo modelo penal de la seguridad ciudadana.** Revista Electrónica de Ciencia Penal y Criminología. 2004, núm. 06-03, p. 07. Disponível em http://criminet.ugr.es/recpc http://criminet.ugr.es/recpc.

_____, José Luis**. De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado.** Revista Electrónica de Ciencia Penal y Criminología. 2005, núm. 07-01, p. 04. disponível em http://criminet.ugr.es/recpc http://criminet.ugr.es/recpc.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DUBASH, Navroz & MORGAN, Bronwen. **Understanding the Rise of the Regulatory State in the Global South**. Regulation & Governance. Oxford: Oxford University Press, 2012

ETZIONI, Amitai, **A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach**.: A Journal of Law and Policy for the Information Society, Vol. 10. 2014. Disponível em SSRN: https://ssrn.com/abstract=2348117.

_____, **A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational**, Brooklin Law Review, Vol. 80. 2015. disponível em http://brooklynworks.brooklaw.edu/blr/vol80/iss4/2

_____. **Privacy in a cyber age : policy and practice**. Studies in Cybercrime and Cybersecurity series. New York: Palgrave Macmillan, 2015.

FERRAJOLI, Luigi. **El Derecho Penal Mínimo.** In. RAMÍREZ, Juan Bustos (dir.) Prevención y teoría de la pena. Santiago de Chile: Editorial Jurídica Conosur, 1995.

_____. **Direito e razão. Teoria do garantismo penal.** 3ª. Edição. São Paulo: Editora Revista dos Tribunais, 2010.

FERGUSON. Andrew Guthrie. **Big data and predictive reasonable suspicion.** University of Pennsylvania Law review. Vol. 163 nº 2. 2015.

_____. **The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement.** 2017.

FRAGOSO, NAthalie e RODRIGUES, Gabriel B. **Protodefesa à brasileira: contraditório e ampla defesa em investigações sigilosas.** Revista de Direito Público, Vol. 18, n. 100. out/dez 2021. pp. 581-605

FRANCISCO, Maria de Fátima Simões. A**ristóteles enquanto fonte das concepções de espaço público e espaço privado de Hannah Arendt.** Notandum, Ano X - N. 14, 2007. Disponível em http://www.hottopos.com/notand14/fatima.pdf.

FRYDMAN, B., HENNEBEL., L. LEWKOWICZ, G.,**Public strategies for internet Co-Regulation in the United States, Europe and China.** *In* BROUSSEAU, E., MARZOUKI, M., e MËADEL, C. **Governance, Regulations and Powers on the the Internet.** Cambridge: Cambridge University Press, 2008. Disponível em HTTP://ssrn.com/abstract=1282826.

GARTNER. **Gartner Glossary. definition of big data.** disponível em: https://www.gartner.com/en/information-technology/glossary/big-data.

GETSCHKO, Demi. **As origens do marco civil da internet.** *In* LEITE, George Salomão e LEMOS. Ronaldo (coords). Marco civil da internet. São Paulo: Atlas, 2014.

GIMBERNAT ORDEIG, Enrique **¿Tiene un futuro la dogmatica juridicopenal?** Madrid: Editorial Civitas, 1984. Disponível em https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080521_84.pdf

GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism.** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** Washington: TechFreedom, 2010. Disponível em https://www.nyu.edu/projects/nissenbaum/papers/The-Next-Digital-Decade-Essays-on-the-Future-of-the-Internet.pdf

GOLDSMITH, Jack L., **Against Cyberanarchy**, Chicago Law Review nº. 1199, 1998.

GONZAGA, Ana Carolina Magalhães e COUTO, Dilnéia Rochana Tavares do. **A dicotomia do público/privado em Hannah Arendt e Jürgen Habermas: interações e reflexões à luz da teoria crítca contemporânea.** Complexitas - Rev. Fil. Tem., Belém, v. 2, n.2 , p. 18-33, jul./dec. 2017.

GRAY, John. **Surveillance Capitalism Vs. The Surveillance State.** Noema Magazine, junho de 2020. Disponível em https://www.noemamag.com/surveillance-capitalism-vs-the-surveillance-state/

GREENWALD, Glenn. **NSA collecting phone records of millions of Verizon customers daily.** disponível em https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

GUARAGNI, Fábio André. **As teorias da conduta em direito Penal.** São Paulo: RT, 2.a Ed. 2010

GUIMARÃES, Juliana Depiné Alves .**Opinião pública e internet: uma discussão acerca do conceito de esfera pública habermasiana nos ambientes digitais.**

HABERMAS, Jürgen. **Historia y crítica de La opinion publica. La transformación estrutural de La vida pública.** 5ª. Edición**.** Barcelona: Ediciones G. Gilli, 1997.

_____. **Direito e democracia: entre facticidade e validade.** Vol. II. Rio de Janeiro: Tempo brasileiro, 1997.

_____. **Direito e Democracia: entre faticidade e validade.** Vol. I, Rio de Janeiro: Tempo brasileiro, 2007

_____. **Mudança estrutural da esfera pública. Investigações sobre uma categoria da sociedade burguesa.** Tradução Denilson Luis Werle. São Paulo: Editora Unesp, 2014.
.

HAFNER, Katie e LYON, Matthew. **Where wizards stay up late (the origins of the internet).** New York: Touchstone, 1998.

HARTZOG, Woodrow. **Privacy´s blueprint. The battle to control the design of new Technologies**. Cambridge: Harvard University Prees, 2018.

HAUTALA, Laura**. The Snowden effect: Privacy is good for business.** Cnet. Disponível em https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/

HASSEMER, Winfried. **Persona, mundo y responsabilidad. Bases para una teoria de la imputación em derecho penal.** Editorial Temis: Santa Fe de Bogotá – Colômbia, 1999.

HERRING, Susan C. **Should You Be Capitalizing the Word 'Internet'?** Wired. outubro de 2015. Disponível em https://www.wired.com/2015/10/should-you-be-capitalizing-the-word-internet/

HIRSCH, Dennis D., **The Glass House Effect: Big Data, The New Oil, and the Power of Analogy**, Maine Law Review, Vol. 66, 2014. Disponível em: https://digitalcommons.mainelaw.maine.edu/mlr/vol66/iss2/3

HOLLAND, Brian. **Section 230 of the CDA:Internet Exceptionalism as a Statutory Construct. .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** Washington: TechFreedom, 2010. Disponível em https://www.nyu.edu/projects/nissenbaum/papers/The-Next-Digital-Decade-Essays-on-the-Future-of-the-Internet.pdf

HOOD, Christopher, ROTHSTEIN, Henry e BALDWIN, Robert.**The Government of Risk: Understanding Risk Regulation Regimes.** Oxford: Oxford University Press, 2001.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICAS. **Pesquisa Nacional por Amostra de Domicílios Contínua**. disponível em: https://www.ibge.gov.br/estatisticas-novoportal/sociais/populacao/17270-pnad-continua.html?edicao=19937&t=resultados

The global state of digital in 2018—from Argentina to Zambia. Disponível em https://hootsuite.com/pt/pages/digital-in-2018

KASPAR, Debbie. **The Evolution (or Devolution) of Privacy**, Sociological Forum, n. 20, 2005. Disponível em http://www.jstor.org/stable/4540882

KEEN, Andrew. **The internet is not the answer.** New York**:** Grove Press, 2015.

KELSEN, Hans. **Teoria Geral das Normas.** Porto Alegre: Sergio Fabris, 1986.

KOZINSKI, Alex e GOLDFOOT, Josh. **A Declaration of the Dependence of Cyberspace. .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** Washington: TechFreedom, 2010. Disponível em https://www.nyu.edu/projects/nissenbaum/papers/The-Next-Digital-Decade-Essays-on-the-Future-of-the-Internet.pdf

KRANZBERG, Melvin. **Technology and History: 'Kranzberg's Laws**. Technology and Culture, vol. 27, no. 3, 1986, pp. 544–560. Disponível em www.jstor.org/stable/3105385 .

_____. **Software for human hardware?** in ZUNDE, Pranas e Hocking, Dan. **Empirical foundations of information and software science.** New York.: Plenum Press, 1990. disponível em https://doi.org/10.1007/978-1-4684-5862-6_1

KRISHNAMURTHY, Vivek. **Cloudy with a Conflict of Laws**. The Berkman Klein Center for Internet & Society Research Publication. 2016. Disponível em SSRN: https://ssrn.com/abstract=2733350 or http://dx.doi.org/10.2139/ssrn.2733350

LEINER, Barry M., CERF, Vinton G. CLARK, David D. et alli. **A brief history of internet.** Internet Society, 1997. Disponível em https://www.internetsociety.org/resources/doc/2017/brief-history-internet/

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2012.

LESSIG, Lawrence. **Code and other laws of cyberspace v. 2.0,** New York: Basic Books, 2006. Disponível em http://codev2.cc/download+remix/Lessig-Codev2.pdf.

LESSIG, Lawrence. **The Future of Ideas: the Fate of the Commons in a Connected World,** New York: Random House: 2001. disponível em http://www.the-future-of-ideas.com/download/lessig_FOI.pdf

LEWIS, James; ZHENG, Denise e CARTER, William. **The effect of encryption on lawfull Access to Communucations and data.** Nova Yok: Rowman & Littlefield, 2017. Disponível em https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE

LOPES JUNIOR, Aury; GLOECKNER, Ricardo Jacobsen. **Investigação Preliminar no Processo Penal**. 5ª ed. São Paulo: Saraiva, 2013, p. 322-323.

LOSEKANN, Cristiana **A esfera pública habermasiana. Seus principais críticos e as possibilidades do uso deste conceito no contexto brasileiro.** Pensamento Plural. 04, 37 - 57, janeiro/junho 2009 Disponível em: http://pensamentoplural.ufpel.edu.br/edicoes/04/02.pdf.

LUBENOW, Jorge Adriano**. A esfera pública 50 anos depois**: esfera pública e meios de comunicação em Jürgen Habermas em homenagem aos 50 anos de Mudança estrutural da esfera pública. **Trans/Form/Ação**, Marília , v. 35, n. 3, p. 189-220, Dec. 2012 . Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-31732012000300010&lng=en&nrm=iso

LUHMANN, Niklas. **El concepto de riesgo** *in* BERIAIN, Josetxo. (comp.) **Las consecuencias perversas de la modernidad. Modenidad, contingencia y riesgo** Barcelona: Anthropos, 1996, p. 144
GRAEF, Aileen. **Elon Musk: We Are "Summoning a Demon" with Artificial Intelligence,** The Economist, UPI edição de outubro de 2014. Disponível em: http://www.upi.com/BusinessNews/2014/10/27/ElonMusk-We-are-summoning-a-demon-with-artificial-intelligence/4191414407652/

LYON, David. **Surveillance**, **Snowden, and Big Data: Capacities, consequences, critique.** Big Data & Society – Jul-Dez 2014. Disponível em http://journals.sagepub.com/doi/abs/10.1177/2053951714541861

_____. **The culture of surveillance. Watching as a way of life**. Cambridge: Polity Press, 2019.

MANKIW. Gregory. **Introdução à economia.** São Paulo: Cengage Learning, 2009.

MAJONE, Giandomenico. **The transformation of the regulatory State.** Osservatorio sull'Analisi de Impatto della regolazione. 2010. Disponível em www.osservatorioair.it

MANIKA, James, CHUI, Michael, BROWN, Brad et alli. **Big data: the next frontier for innovation, competition, and produtivity.** McKinsey Global Institute, 2011. Disponível em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation#

MARSDEN, Christopher. **Information and communications technologies, globalization and regulation.** in MARSDEN, Christopher (org). **Regulating the Global Information Society.** Londres: Routledge, 2000.

MARSDEN, Christopher. **Internet co-regulation: european Law, regulatory governance and legitimacy.** Cambridge: Cambridge University Press, 2011.

MARX, Gary T. **Whats's new about new surveillance'? Classifying for change and continuity.** in Hier, Sean e Greenberg, Josh. **The surveillance studies reader.** New York: McGraw-Hill. 2007.

_____. **"Yous papers, please": personal and professional encounters with surveillance.** in BALL, Kirstie, HAGGERTY, Kevin e LYON, David. **Routledge handbook of surveillance studies.** New York: Routledge, 2014.

TAIT, Matt. **Decrypting the Going Dark Debate.** Lawfare, 2017. Disponível em https://www.lawfareblog.com/decrypting-going-dark-debate

MAYBIN, Simon. **Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA.** BBC News, 31 outubro de 2016. Disponível em https://www.bbc.com/portuguese/brasil-37677421

MAYER-SCHONBERGER, Viktor e CUKIER, Kenneth. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**. Rio de Janeiro : Elsevier, 2013.

_____, Kenneth.**The rise of big data. How it's chancing the way we think about the world.** Foreign affairs. may/jun 2013. disponível em : https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data

MCLUHAN GALAXY. **A Schoolman's Guide to Marshall McLuhan by John Culkin, S.J., 1967.** disponível em: https://mcluhangalaxy.wordpress.com/2017/09/19/a-schoolmans-guide-to-marshall-mcluhan-by-john-culkin-s-j-1967/

MENDES, Gilmar Ferreira e BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 8ª. Ed. São Paulo: Saraiva, 2013.

MEDEIROS, Henrique. **Nunca as leis de Asimov estiveram tão presentes, diz especialista em direito digital.** Mobiletime, 3/10/18 21:52. disponível em https://www.mobiletime.com.br/noticias/03/10/2018/nunca-as-leis-de-asimov-estiveram-tao-presentes-diz-especialista-em-direito-digital/

MELLADO, Jose Maria Asencio. **Los informes de inteligencia policiales. su influencia en los principios esenciales del proceso penal** *in* PEREIRA, Flavio Cardoso (org.) **Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo**. Brasilia, DF : Gazeta Juridica, 2016.

MORGAN, Bronwen e YEUNG, Karen. **An introduction to Law and regulation.** Cambridge: Cambridge University Press, 2007

MOROZOV, Evgeny. **The Real Privacy Problem.** MIT Technology review. Outubro de 2013. disponível em **https://www.technologyreview.com/2013/10/22/112778/the-real-privacy-problem/**

MOROZOV. Evgeny. **Big tech. A ascensão dos dados e a morte da política.** São Paulo: Ubu Editora. 2018.

MOURA, Maria Thereza de Assis. **A ilicitude na obtenção da prova e sua aferição**. Palestra proferida no I Seminário no Estado de Minas Gerais – V Seminário Regional do IBCCRIM- Uberlândia, no dia 5 de dezembro de 1997. Disponível em www.ambitojurídico.com.br

MUELLER, Milton. **Networks and States**. The global politics of internet governance. 2010

MURRAY, Andrew. **Nodes and gravity in virtual space.** 5 Legisprudence 195, 2011**.**

MURRAY, Andrew. **The regulation of cyberspace, Control in the online environment.** 2007.

NISSENBAUM, Helen. **Protecting privacy in a information age: the problem of privacy in public**. Law and Philosophy, 1998. Disponível em SSRN: https://ssrn.com/abstract=139144.

_____. **Privacy in context. Technology, policy and the integrity of social life.** Stanford: Stanford Law Book, 2010. Ainda NISSENBAUM, Helen. **Protecting privacy in a information age: the problem of privacy in public**. Law and Philosophy, 1998. Disponível em https://ssrn.com/abstract=139144.

_____. **Privacy in context. Technology, policy and the integrity of social life** Stanford Law Books: Stanford, 2010.

OLIVEIRA, Elizandro e REIS, Jaime. **O poder nas corporações de ofícios.** Anais do VIII Congresso Internacional de História. 2017. Disponível em http://www.cih.uem.br/anais/2017/trabalhos/3493.pdf

OLIVEIRA, Vânia Aparecida Rezende de. **Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa**. Cad. EBAPE.BR, Rio de Janeiro , v. 8, n. 4, p. 782-788, 2010. Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1679-39512010000400013&lng=en&nrm=iso

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Disponível em https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OCDE privacy framework.** 2013. Disponível em : http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf

OSOBA, Osonde A e WELSER IV, William. **The Risks of Artificial Intelligence to Security and the Future of Work**. 2017. Disponível em https://www.rand.org/pubs/perspectives/PE237.html

PARLAMENTO DO REINO UNIDO. **Churchill and the Commons Chamber. disponível** em https://www.parliament.uk/about/living-heritage/building/palace/architecture/palacestructure/churchill/

PETERSON, Andrea. **Your location history is like a fingerprint. And cops can get it without a warrant.** The Washington Post. 30 de julho de 2013. Disponível em https://www.washingtonpost.com/news/the-switch/wp/2013/07/31/your-location-history-is-like-a-fingerprint-and-cops-can-get-it-without-a-warrant/

POST, David e JOHNSON, David. **Law and Borders–The Rise of Law in Cyberspace**, Stanford Law Review, nº 48, 1996. Disponível em http://journals.uic.edu/ojs/index.php/fm/article/view/468/824

PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO . **Relatório de desenvolvimento humano 2019.** Deisponível em http://hdr.undp.org/sites/default/files/hdr_2019_overview_-_pt.pdf

PROSSER, Tony. **Theorising Utility Regulation.** Heinonline, 62 Mod. L. Rev. 196. 1999

_____. **Two visions of regulation.** Paper by Tony Prosser for 'Regulation in the Age of Crisis', University College. Dublin, 2010. Disponível em http://regulation.upf.edu/dublin-10-papers/1H1.pdf

RICHARDS, Neil M. **Four Privacy Myths.** in SARAT, Austin (org). **A world without privacy : what law can and should do?** 2015

RICHARDS, Neil. M. **The iPhone case and the future of civil liberties.** Boston Review, February 25, 2016. Disponível em https://www.bostonreview.net/us/neil-richards-apple-iphone-privacy.

RICHARDS, Neil. e KING, Jonathan. **Three paradoxes of big data.** Stanford Law Reviewonline Vol. 66:41. Disponível em https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_StanLRevOnline_41_RichardsKing.pdf

RODAS, Sérgio. **França proíbe divulgação de estatísticas sobre decisões judiciais.** Conjur, 5 de junho de 2019. Disponível em https://www.conjur.com.br/2019-jun-05/franca-proibe-divulgacao-estatisticas-decisoes-judiciais

RODOTÀ, Stefano. **A vida na sociedade da vigilância - a privacidade hoje.** Rio de Janeiro: Renovar, 2008.

ROXIN, Claus. **Derecho Penal**. **Parte general.** Fundamentos. La estructura de la teoría del delito. Madrid: Civitas, 1997. p. 207.

SANCHEZ, Jesus Maria Silva. **A expansão do Direito Penal.** 2a. edição. São Paulo: Revista dos Tribunais, 2010.

SANCHIS, Luis Prieto. **El juicio de ponderación constitucional.** In CARBONELL, Miguel (org.). El principio de proporcionalidad y la interpretación constitucional**.** Quito: Ministerio de Justicia y Derechos Humanos, 2008.

SARMENTO, Daniel. **Livres e Iguais: Estudos de Direito Constitucional**. São Paulo: Lúmen Juris, 2006, p. 200.

SASKEN, Sassia. **Losing Control?: Sovereignty in an Age of Globalization.** New York: Columbia University Press, 1996. Disponível em https://www.researchgate.net/publication/30529999

_____. **Towards a Sociology of Information Technology** - Current Sociology, Maio de 2002, Vol. 50(3): 365–388 disponível em http://www.saskiasassen.com/PDFs/publications/Towards-a-Sociology-of-Information-Technology.pdf

SCHERER, Matthew. **Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies**, 29 HARV. J. L. & TECH. 353,201

SHAH, N., BHAGAT, N. e SHAH, M. **Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention**. *Vis. Comput. Ind. Biomed. Art.* 09 de abril de 2021. disponível em https://doi.org/10.1186/s42492-021-00075-z

SILVA, Virgílio Afonso da. **Direitos fundamentais. Conteúdo essencial, restrições e eficácia.** 2ª. ed. São Paulo: Malheiros, 2010.p. 46.

SILVA, Filipe Carreira da. **Habermas e a esfera pública: reconstruindo a história de uma ideia**. Sociologia, Problemas e Práticas, Oeiras , n. 35, p. 117-138, abr. 2001 . Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0873-65292001000100006&lng=pt&nrm=iso>. acessos em 04 maio 2020.

SIMITIS, Spiros. **Reviewing privacy in an information society.** University of Pennsylvania Law Review. Vol. 135, n. 3. 1987. p. 732. Disponível em www.jstor.org/stable/3312079.

SOLOVE, Daniel J. **Digital Dossiers and the Dissipation of Fourth Amendment Privacy,** 75 South California Law. Review. 2002. Disponível em https://scholarship.law.gwu.edu/faculty_publications/943/

_____. **Conceptualizing privacy.** California Law Review, vol. 90. 2002**.**

_____. **Understanding privacy.** Cambridge: Harvard University Pres, 2008. Disponível em http://ssrn.com/abstract=1127888.

_____. **Nothing to hide. The false tradeoff between privacy and security.** New Haven: Yale University Press, 2011

STALLA-BOURDILLON, Sophie; PHILLIPS, Joshua e RYAN, Mark D. **Privacy vs. Security**, 2015.

SOLUM, Lawrence B. e CHUNG, Minn. **The Layers Principle: Internet Achitecture and the Law**, Notre Dame Law Review, vol. 815, 2004. Disponível em http://scholarship.law.nd.edu/ndlr/vol79/iss3/1

SUNSTEIN, Cass. **Laws of fear: beyond precautionary principle.** Cambridge: Cambridge University Press, 2005.

_____. **Para além do princípio da precaução**. Revista de Direito Administrativo, V. 259. Rio de Janeiro: Ed. Revista dos Tribunais, 2012.

STEWART, Richard B. **Environmental regulatory decisionmaking under uncertainty**. University College London Symposium on the Law & Economics of Environmental Policy, 2001. Disponível em http://www.ucl.ac.uk/cserge/Stewart.pdf. Acesso em 20/07/2015.

SVANTESSON, Dan. **The times they are a-changin' (every six months)-- The challenges of regulating developing technologies**. Law papers. disponível em https://www.researchgate.net/publication/27827337

TARUFFO, Michele. **Uma simples verdade. O juiz e a reconstrução dos fatos.** São Paulo: Marcial Pons, 2012.

THE GUARDIAN. **TechScape: can AI really predict crime?** 22 de dezembro de 2021. Disponível em https://www.theguardian.com/technology/2021/dec/22/techscape-lapd-operation-laser

THOMPSON, Derek. **Google's CEO: 'The Laws Are Written by Lobbyists'. Eric Schmidt on the power of lobbyists, a Google "implant", and how China resembles a big business.** Disponível em https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

UNIÃO EUROPEIA. **RGPD**. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1

VAN EETEN Michel e MUELLER, Milton. **Where is the governance in Internet governance?** New Media & Society, 2012. Disponível em https://www.researchgate.net/deref/http%3A%2F%2Fnms.sagepub.com%2Fcontent%2Fearly%2F2012%2F11%2F19%2F1461444812462850.

VIGO, Rodolfo. **Balance de la teoría jurídica discursiva de Robert Alexy**. Doxa - Cuadernos de Filosofía del Derecho. Nº 23, p. 203-224. Disponível em <*http://publicaciones.ua.es/filespubli/pdf/02148676RD44747684.pdf*>

WARREN, Samuel D e BRANDEIS, Louis D. **The Right to Privacy**. 1890. Disponível em https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

WEBSTER, Frank. **Theories of information society**, 4ª. Ed. Londres: Routledge, 2014.

WESTIN, Alan. **Privacy And Freedom**, New York: Ig Publishing, 1967. (Ebook)

WIENER, Jonathan B., **The regulation of technology, and the technology of regulation.** Technology in Society nº 26, 2004. p. 483–500. Disponível em http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1960&context=faculty_scholarship

WERTHEIN, Jorge. **A sociedade da informação e seus desafios,** disponível em http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf.

WILSON III, Ernest. **The Information Revolution and Developing Countries**. Londres: Routledge, 2004.

WOLFENSOHN, James D. **Development and international cooperation in the twenty-first century : the role of information technology in the context of a knowledge-based global economy (ECOSOC).** 2000. Disponível em http://documents.worldbank.org/curated/en/519081467994605225/Development-and-international-cooperation-in-the-twenty-first-century-the-role-of-information-technology-in-the-context-of-a-knowledge-based-global-economy-ECOSOC-by-James-D-Wolfensohn-President

WORLD ECONOMIC FORUM. **Data science in the new economy: a new race for talent in the fourth industrial revolution.** Julho de 2019. disponível em https://www.weforum.org/reports/data-science-in-the-new-economy-a-new-race-for-talent-in-the-fourth-industrial-revolution

WORLD WIDE WEB CONSORTIUM (W3C). **Frequently asked questions.** Disponível em https://www.w3.org/People/Berners-Lee/FAQ.html

WORLD WIDE WEB CONSORTIUM. **HTML 4.01 Specification.** Disponível em https://www.w3.org/TR/html401/struct/links.html#h-12.1

WU, Tim. **Is Internet Exceptionalism Dead? .** In SZOKA, Berin e MARCUS, Adam. **The next digital decade - Essays on the future of the internet.** Washington: TechFreedom, 2010. Disponível em https://www.nyu.edu/projects/nissenbaum/papers/The-Next-Digital-Decade-Essays-on-the-Future-of-the-Internet.pdf

YEUNG, Karen. **Algorithmic regulation: A critical interrogation**. Regulation & Governance. 12. 10.1111/rego.12158. 2017

ZAVRŠNIK, Ales. **Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?** Journal of Contemporary European Research. vol. 9, 2013. pp. 181-202. disponível em https://www.jcer.net/index.php/jcer/article/view/452

ZITTRAIN, Jonathan. **The Future of the Internet and How to Stop It. The Future of the Internet - And How to Stop It.** New HAven: Yale University Press, 2008. Disponível em: http://ssrn.com/abstract=1125949

ZITTRAIN, Jonathan L., OLSEN, Matthew G., O'BRIEN, David e SCHNEIER, Bruce. **Don't Panic: Making Progress on the "Going Dark" Debate**.". Berkman Center Research Publication, 2016. Disponível em http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552576

ZUBOFF, Shoshana. ***Big other:*** **capitalismo de vigilância e perspectivas para uma civilização de informação.** in BRUNO, Fernanda et al. **Tecnopolíticas da vigilância. perspectivas da margem.** São Paulo: Boitempo, 2018.

_____. **The age of surveillance capitalism: The Fight for a Human Future at the New Frontier of Power**, 2019