Painel-Proteção de dados, Fluxo Transnacional, GDPR e novos padrões

Conference Paper · January 2018

CITATIONS
0

READS
73

1 author:

Bruno Bioni
University of São Paulo
20 PUBLICATIONS **8** CITATIONS

SEE PROFILE

III SEMINÁRIO

GOVERNANÇA DAS REDES

POLÍTICAS, INTERNET E SOCIEDADE

ORGANIZADORES
FABRÍCIO BERTINI PASQUOT POLIDO
LUCAS COSTA DOS ANJOS
LUÍZA COUTO CHAVES BRANDÃO

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

III SEMINÁRIO

GOVERNANÇA DAS REDES

POLÍTICAS, INTERNET E SOCIEDADE

ORGANIZADORES

FABRÍCIO BERTINI PASQUOT POLIDO
LUCAS COSTA DOS ANJOS
LUÍZA COUTO CHAVES BRANDÃO

S471a Seminário Governança das Redes (3.: 2018 : Belo Horizonte, MG).
Anais do III Seminário Governança das Redes [recurso eletrônico]: políticas, internet e sociedade / Fabrício Bertini Pasquot Polido, Lucas Costa dos Anjos, Luiza Couto Chaves Brandão, organizadores. – Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018.
Recurso online: PDF (435 p.: il.).
Inclui bibliografias.
ISBN: 978-85-94202-03-1.

1. Direito 2. Direito internacional 3. Direito internacional privado 4. Direito comparado 5. Internet 6. Internet – Aspectos jurídicos 7. Direito à privacidade 8. Cibercultura 9. Propriedade intelectual 10. Globalização 11. Big data I. Polido, Fabricio Bertini Pasquot II. Anjos, Lucas Costa dos III. Brandão, Luíza Couto Chaves IV. Título

CDU(1976) 34:007

Ficha catalográfica elaborada pelo bibliotecário Junio Martins Lourenço CRB 6/3167.

Projeto gráfico: Felipe Duarte
Capa: Felipe Duarte
Diagramação: Felipe Duarte
Revisão: Davi Teófilo, Gustavo Rodrigues, Lahis Kurtz, Lucas Anjos e Mariana Lopes
Finalização: Felipe Duarte

III SEMINÁRIO

GOVERNANÇA DAS REDES

POLÍTICAS, INTERNET E SOCIEDADE

Instituto de Referência em Internet e Sociedade

DIREÇÃO

Luíza Couto Chaves Brandão

VICE-DIREÇÃO

Odélio Porto Jr.

CONSELHEIROS CIENTÍFICOS

Fabrício Bertini Pasquot Polido
Lucas Costa dos Anjos

MEMBROS

Davi Teofilo / Pesquisador
Felipe Duarte / Comunicação
Gustavo Rodrigues / Pesquisador
Lahis Kurtz / Pesquisadora
Mariana Lopes / Pesquisadora
Paloma Rocillo Rolim do Carmo / Pesquisadora
Pedro Vilela Resende Gonçalves / Co-fundador e pesquisador
Victor Barbieri Rodrigues Vieira / Pesquisador

Organização

Apoio

SUMÁRIO

PARTE II - GRUPOS DE TRABALHO

Bruno Bioni (Data Privacy e NIC.br)

Boa tarde todos e todas, gostaria de agradecer o convite feito pelo IRIS para estar aqui hoje conversando com vocês sobre proteção de dados, fluxo transnacional, GDPR e novos padrões. O IRIS tem sido um ator fundamental na produção de pesquisa de temas relacionados à governança da internet e, principalmente relacionado à proteção de dados pessoais. Por isso, estar nesse congresso, realizado na Faculdade de Direito da UFMG, é um momento especial para aquecer essas discussões e ao mesmo tempo fazer uma reflexão crítica sobre como o debate da proteção de dados pessoais está posto no Brasil.

Meu nome é Bruno Bioni, professor e fundador do Data Privacy Brasil e hoje falo na minha capacidade acadêmica. Nos meus 30 minutos, eu pretendo endereçar a questão que o título desse painel nos provoca a responder. Ao usar a expressão novos padrões, o mote dessa mesa nos convida a pensar se existe, primeiro, algo de novo no campo da proteção dos dados pessoais, e, segundo, se há emergência de algo novo e hegemônico – por isso, o termo padrão. E, havendo esses novos padrões, como o Brasil está posicionado: nosso quadro regulatório é convergente a esses padrões?

Para ensaiar uma resposta, eu vou dividir a minha fala em dois eixos. E, antes de mais nada, eu não vou usar o termo padrões, ou quando usá-la, farei no sentido atécnico da palavra porque eu não reuni evidências empíricas que apontem algum modelo hegemônico e, portanto, prevaleceria sobre outros. Por isso, é importante dar um passo para trás e investigar algo menos ambicioso: Há uma nova lógica, uma nova racionalidade, em termos de regulação na arena da proteção à privacidade e aos dados pessoais? Se sim, o Brasil adotou essa racionalidade na sua nova lei geral de proteção de dados pessoais? Quais são os desafios e as particularidades do contexto brasileiro para implementar de forma eficiente essa nova racionalidade regulatória, isto é, o seu enforcement?

Viktor Mayer-Schönberger é muito conhecido pelo seu livro sobre direito ao esquecimento – Delete: The Virtue of Forgetting in the Digital Age –, mas ele tem um outro texto, na minha opinião um dos seus melhores, em que analise o progresso geracional de leis de proteção de dados pessoais. Ao remontar tal evolução histórica, o resultado é o mapeamento de, ao menos, 4 (quatro) gerações de leis de proteção de dados pessoais com ênfase no cenário europeu.

A racionalidade da primeira geração era praticamente de "domesticar" a tecnologia, de modo que as primeiras leis buscaram prescrever taxativamente quais seriam os usos lícitos e ilícitos com dados pessoais dos cidadãos. Não demorou muito para que tal estratégia se mostrasse falha, na medida em que não se mostrou escalável e factível para o legislador acompanhar e sincronizar a sua produção legislativa ao progresso tecnológico.

Como decorrência do insucesso dessa primeira geração, surgem a segunda e a terceira geração de leis de proteção de dados pessoais. Já não se procura prever ex ante toda gama de usos possíveis com os dados, prevendo-se, por outro lado, os direitos e deveres de todos os atores do ecossistema. É justamente esse o âmago das chamadas Fair Information Practices Principles/FIPs, cuja tradução literal do termo permite apontar para a articulação de princípios que norteiam práticas justas e, assim, catalisar confiança de todos os atores do ecossistema. Diferentemente da primeira geração de

leis, a regulação não diz de antemão quais são os tratamentos lícitos e ilícitos com dados pessoais, deixando espaço para que floresçam novos modelos de negócio e formação de políticas públicas, desde que observem os direitos e deveres previstos na legislação. Os direitos clássicos de proteção de dados pessoais, chamados de ARCO datam dessa geração de leis de proteção de dados pessoais: a)acesso; b)retificação; c)correção e; d) oposição.

A terceira e quarta geração completam o quadro de direitos e dos atores de um arranjo de governança de dados. Respectivamente: i) um dos direitos que se consolida e ganha protagonismo é a participação do cidadão no fluxo das suas informações através do consentimento, de modo que ele as autodeterminasse (autodeterminação informacional); ii) ao mesmo tempo, reconhece-se uma assimetria de poder e de informação entre o cidadão e quem processa seus dados, constituindo-se, então, um modelo de fiscalização e aplicação das leis cuja sua vértebra são autoridades estatais com expertise e missão institucional voltadas a fazer valer o conjunto de normas previsto em tais leis.

Essas quatro gerações de leis de proteção de dados pessoais consistem na primeira fase de uma racionalidade regulatória do campo das leis de proteção de dados pessoais, cuja melhor expressão são: a convenção 108 do Conselho da Europa; as diretrizes da Organização para o Desenvolvimento Socioeconômico/OCDE e; a Diretiva 94/95 da União Europeia. Esse período, de 1973 à 1995, é marcado pelo alto grau de convergência dessas instrumentos normativos, todos eles estruturados em arquitetar os direitos e deveres de todos os agentes de governança de dados, especialmente no que diz respeito à perspectiva de se franquear aos cidadãos controle sobre seus dados e a introjeção de autoridades para a efetiva aplicação desse conjunto de regras.

Do ano 2000 em diante, esses três instrumentos foram modernizados. Respectivamente: i) em 2013, a OCDE emitiu suas novas guidelines; o privacy framework; iii) em 2014, a União Europeia concluiu o texto do Regulamento Europeu de Proteção de Dados pessoais; iii) em 2016, o Conselho da Europa modernizou a convenção internacional 108 de proteção de dados pessoais. Toda essa movimentação é simbólica no sentido de que algo está acontecendo no campo da proteção de dados pessoais, o que corresponde justamente a uma nova racionalidade regulatório nessa arena.

Há uma virada "copernicana" que nos induz necessariamente a refletir e diagnosticar o que significa essa ebulição normativa, sobretudo como um primeiro passo para verificar se há, de fato, "novos padrões" de proteção de dados pessoais.

Para verificar se há uma nova racionalidade regulatória, serão analisados como os três elementos mais importantes de qualquer lei de proteção de dados pessoais foram repaginados nesse movimento de modernização. Se, ao final, for possível diagnosticar uma mudança dessa espinha dorsal, então a resposta tende a ser afirmativa sobre a existência de uma nova racionalidade regulatória, fornecendo-se, ainda, uma moldura analítica para investigações futuras e, sobretudo, o que se pode esperar durante a aplicação e fiscalização dessas "novas" leis de proteção de dados pessoais – novos padrões.

Se resgatarmos a aplicação da primeira fase das leis e normas de proteção de dados pessoais, verificamos que o conceito de dado pessoal e dado anonimizado era algo como se fosse "preto no branco". Ou seja, não era tão complexo precisar o escopo

de aplicação de leis de proteção de dados pessoais, o que estaria debaixo do seu "guarda chuva". Normativamente e semanticamente fazia muito sentido manter essa dicotomia dura entre dado pessoal e dados anônimos, ou seja, aqueles dados que não tem cara nem rosto, que não podem identificar um sujeito.

Contudo, a partir do surgimento de tecnologias como inteligência artificial, big data, entre outras, essa era dicotomia muito preto no branco vai se tornando mais cinzenta. Hoje, com essas novas tecnologias, há cada vez mais intersecções entre dados pessoais e dados anônimos, não sendo sempre possível cravar preto no branco o que é um ou outro. Não é algo tão simples assim de ser respondido. Se, por exemplo, verificamos a aplicação da tecnologia de big data, alguns engenheiros, quase por diversão, reidentificam e revertem recorrentemente processos de anonimização. É falaciosa a afirmação de que existe uma base de dados ser 100% anônima e útil, na medida em que sempre há um risco residual.

O cientista da computação, Arvind Narayanan, afirma que basta apenas 33 bits de informação para reverter uma base de dados anonimizados. 33 bits é muito pouco, é o nosso nome e mais algum pedaço de informação que eventualmente demos ao fazer o cadastro para entrar nesse prédio. Ou seja, é muito pouco, para cruzar informações e chegar em uma pessoa eu preciso de muito pouca informação, essas novas tecnologias transformaram essas dicotomias – dado pessoal e dado anonimizado - quase em inexistentes.

Um outro estudo que tangibilizar essa questão foi conduzido por engenheiros do MIT, o que eles fizeram? eles pegaram os dados anonimizados de vários cartões de crédito, não tinha a princípio ali nome, endereço, ou algo do tipo, mas esse padrão de consumo revelava onde essas pessoas compraram produtos e serviços, quais os valores dessas compras e a localidade disso tudo. Com base nesse o padrão de consumo, houve a identificação de todos os consumidores dessa base de dados, de modo que os dados anônimos de cartão de crédito não seriam tão anônimos assim.

Essas novas tecnologias são a mola propulsora para termos esse quadro de atualização, de emergência de novos padrões, por assim dizer, que estamos presenciando agora, GDPR, modernização da convenção do Conselho da Europa, das diretrizes da OCDE, e assim por diante. O legislador já não consegue prescrever preto no branco o que é dado pessoal e o que é dado anonimizado, havendo sempre um risco residual nisso tudo.

O segundo ponto é o consentimento, que sempre foi um dos pilares de proteção de dados pessoais, consentimento, dentro daquela lógica de progresso geracional de leis de proteção de dados pessoais, o legislador disse, olha, eu não consigo prescrever de antemão quais são os usos ilícitos e lícitos, então, irei delegar ao próprio titular da informação, é ele que deve exercer esse tipo de controle, é ele que deve autodeterminar suas informações pessoais, vamos encontrar esse "palavrão" em muitos livros, autodeterminação informacional, é isso que significa. E como eu faço isso? o cidadão vai ter que autorizar qualquer tipo de tratamento dos seus dados, para isso temos a figura do consentimento, então ele foi a primeira "carta coringa regulatória" das leis de proteção de dados pessoais.

No entanto, existem diversas tecnologias que permitem inúmeros usos possíveis. Hoje eu coleto um dado, eu enxergo uma determinada finalidade, ma, pode ser que

daqui há dois meses eu enxergue uma outra finalidade ao cruzar com outras bases de dados e encontrar mais informações. Nesse uso intensivo e cada vez mais subsequente desses dados, como que o cidadão controla esse tipo de informação? Em última análise, ele não vai ter poder para racionalizar todos os processos de tomada de decisão.

Por isso, o legislador criou quase como se fosse uma outra carta coringa regulatória que o Guilherme já mencionou aqui: o legítimo interesse. Existem situações nas quais você não irá precisar pedir a autorização do titular dos dados para reutilizar o dado, você pode fazer isso porque se trata de legítimo interesse, mas o que seria esse legítimo interesse? Diante desse conceito jurídico indeterminado, nada mais lógico do que que prever testes em que se realize um balanço e um equilíbrio de quem trata esses dados, dos modelos de negócio, e das legítimas expectativas do cidadão.

Em resumo, ao longo de todo esse progresso geracional de leis de proteção de dados pessoais, eu já não consigo cravar preto no branco, por exemplo, o que é um dado pessoal, um dado anonimizado, quando um dado está sendo tratado, como por exemplo, no legítimo interesse e eu sei que os direitos e as liberdades do cidadão estão sendo garantidos, por exemplo. Trata-se de um cenário de extrema assimetria de informação, tanto o cidadão quanto o órgão regulador. Muitos atores desse ecossistema não conseguem ter toda essa fotografia dos fluxos de dados, quem sabe melhor do que eles é quem está no “chão da fábrica” lidando com esses dados: os próprios agentes econômicos.

Com isso, há cenários cada vez mais incertos, riscos que eu não consigo de certa maneira mapear e identifica-los, sendo este um contexto e conteúdo desafiador para a regulação. O próprio Estado e o órgão regulador, os próprios cidadão começam a olhar e ter o diagnóstico de que não é mais possível alcançar uma regulação efetiva que não conte com um atuação cooperativa dos próprios agentes econômicos. É necessário, portanto, uma nova racionalidade regulatória, o que me parece ser os novos padrões de proteção de dados pessoais.

Abandona-se uma ótica forte que ainda no Brasil é muito presente, de o Estado ser o órgão regulador e que de “cima para baixo” vai emitir quais são as regras do jogo, o que pode ser feito ou não, como se agências reguladoras fossem dar conta do mercado que elas regulam, como se fossem plenamente autossuficientes. Pelo contrário, migra-se para uma outra lógica e uma nova racionalidade de regulação que eu vou falar aqui em termos de meta-regulação ou regulação responsiva. O que quer dizer com essa palavrão? o que é meta-regulação e como ela se diferencia dessa racionalidade de comando e controle?

Meta-regulação, se formos pegar principalmente os cientistas políticos, econômicos e, assim por diante, eles falam: olha, existe alguma coisa aqui que é o meio do caminho do que vínhamos olhando como uma falsa dicotomia, ou seja, o Estado de um extremo regulando tudo, dizendo tudo que pode ser feito e, do outro, quase como se fosse uma autorregulação, apenas os próprios agentes econômicos, principalmente o setor privado, se auto regulando. Existe um meio termo aqui, que seria a ideia de meta-regulação, uma nova racionalidade.

De certa forma, eu, Estado, consigo delegar e pedir para que os próprios agentes econômicos também executem tarefas regulatórias que, antes, seriam próprias do agente regulador ou do Estado. Eu consigo, de certa maneira, prescrever quais são os

objetivos, o tipo ideal do que eu quero atingir com a regulação, sendo que os meios para se chegar nesses objetivos serão delegados aos próprios agentes econômicos, de modo que eles terão discricionariedade para atingir esses objetivos, essas metas previstas nas legislações.

Nesse sentido, alguns doutrinadores vão até usar o termo auto regulação regulada, algo que é uma sopinha de palavras, mas que tenta identificar e passar esse tipo de perspectiva. O que fica claro é que quem vai ser o regulador, quem vai ter essa tarefa, não vai ser apenas o Estado, mas serão os próprios agentes econômicos, entidades de classe, terceiros como entidades certificadoras e assim por diante.

É exatamente isso que estamos vendo ser atualizado naquelas leis e normas de proteção de dados pessoais, principalmente a partir dos anos 2000. Façam o exercício vocês mesmos, compararem a GDPR com a antiga diretiva, as principais inovações são os capítulos de relatórios de impacto à proteção de dados pessoais, códigos de boas condutas, selos e assim por diante. O que eu quero endereçar é que temos um cenário de cada vez mais de flexibilidade, em que o Estado cada vez menos tem o poder de antemão prescrever o que pode ou não ser feito de forma binário em uma lógica de comando e controle.

Com isso, delega-se para os agentes econômicos certas tarefas regulatórias. Esse cenário de uma cenário regulação cada vez mais flexível vem acoplado com a estratégia em verificar como cada setor ou certos atores regulados vão reagir bem ou mal com para atingir as metas da regulação. Isso será decisivo para calibrar medidas sancionatórias. Se por exemplo, eu vejo que um determinado setor tem um código de boas condutas que está sendo implementado e, sobretudo, que alguns atores adotaram esses códigos de boas condutas. Mesmo que as condutas delas sejam questionáveis, suscetível de punição, o órgão regulador tende a dizer: eu não vou de “primeira mão” multar, talvez algum tipo de advertência.

Ou seja, eu, órgão regulador, vou atuar muito na lógica de premiar bons comportamentos e não só de reprovar maus comportamentos. Essa é uma mentalidade regulatória nova que traz muito mais flexibilidade, digamos assim.

Nesse sentido, vejam essa tabela em que OCDE, GDPR, Convenção 108 e a nossa Lei Brasileira de Proteção de dados pessoais, todas elas focam muito na ideia de accountability, que foi traduzido para nossa lei de proteção de dados como princípio da responsabilização e demonstração de esforços, nesse sentido, prestação de contas. Ao mesmo tempo, a nossa LGDP prevê um capítulo sobre códigos de boa conduta, o que é algo relativamente novo no nosso ordenamento jurídico se formos comparar com outras leis.

Portanto, a arena de proteção de dados pessoais nos coloca a refletir sobre essa nova racionalidade regulatória que impactará todos os setores da economia. Saúde, varejo, aviação, todos os setores hoje em dia lidam com dados. Um órgão regulador ou punhado deles dão conta de toda essa agenda de regulação? Não, não tem como, não há braços, mesmo que diversas agências sejam bem aparelhadas para isso. É, nesse contexto, que faz ainda mais sentido essa nova racionalidade regulatória cujo resultado final é convidar quem está desenvolvendo, quem está com a mão na massa, projetando seus produtos e serviços, me diz quais são os riscos envolvidos na sua atividade.

Nesse sentido, a nossa lei e a GDPR têm disposições sobre relatórios de impacto

à proteção de dados pessoais. De forma bem franca, esse movimento acena para o seguinte: eu, regulador, não consigo de antemão dizer quais são os riscos, você, agente econômico, tem mais informação e conhecimento do que eu, então você será convidado a fazer isso. Por isso, há emergência de diversas normas relacionados a esse dever de emissão de relatórios de impacto a proteção de dados pessoais.

Mas, Bruno, isso ainda é muito genérico, muito amplo, como irei tangibilizar quais são os riscos próprios de determinados setores? Para isso servem os códigos de boas condutas, com certeza, o risco no setor de saúde é diferente do risco do setor varejista, com certeza o risco do setor automobilístico com carros autônomos é diferente do risco em um mercado aéreo, por exemplo. Então, você, setor – agente econômico, tangibiliza para mim – órgão regulador – todos esses conceitos jurídicos indeterminados e metas da legislação. Por exemplo, o que é legítimo interesse dentro do seu setor? O que é um risco razoável de reversão em um processo de anonimização? Tangibiliza isso.

A legislação começa a convidar esses agentes econômicos para cooperarem e, mais do que isso, criar espaço para que terceiros validem de maneira imparcial tudo isso e seja um longa manus do órgão regulador? Quem são terceiros que poderiam certificar, dar selos? Seu código de boa conduta é tão bom que terá um selo de uma consultoria, um terceiro, que irá certificar essas práticas, se são realmente boas.

Ao final e ao cabo, é possível pensar em um ecossistema, em que cada vez mais, a concepção desses produtos e tecnologias vão embebedar a privacidade como um elemento core deles, é o que tanto falamos como privacy by design e cada vez mais aflorando programas corporativos sobre proteção de dados pessoais. Ou seja, estamos vivenciando um momento, digamos assim, muito caro e eu acho que é essa a importância de estarmos em uma faculdade. Vocês, enquanto pesquisadores, graduandos, olharem para esse novo momento, sim: é tudo muito novo, trata-se de uma agenda de pesquisa para os próximos anos, mas ainda estamos trabalhando nisso tudo para desvendar quais são os impactos dessa nova racionalidade regulatória.

Não se enganem, vai afetar relações de consumo, relações de trabalho e outros tipos de ordenamentos que nem temos ideia quais são ainda.

Para não ficar no plano abstrato e teórico e para terem uma dimensão de que isso já está acontecendo com a GDPR, essa ação é muito curiosa, principalmente em termos de estratégia processual. Nela se juntaram um ativista e um acadêmico que querem entender melhor como funciona a indústria de publicidade digital, especificamente quais são os padrões estabelecidos por essa entidade de associação – IAB Europa – desde que a GDPR entrou em vigor. A IAB Europa criou novos padrões a serem seguidos pela indústria de targeted ads, no entanto os demandantes consideram que o monitoramento ainda é intrusivo e pervasivo e, sobretudo, que há uma falha no design da indústria como um todo. Os novos padrões ainda assim não permitiriam aos usuários ter controle sobre seus dados pessoais, um controle efetivo.

O mais interessante desse caso é a estratégia processual e consequentemente os seus respectivos pedidos. Esses dois caras não pediram para a autoridade de proteção de dados pessoas multar - “cortar a cabeça” dessa prática. Pelo contrário, os pedidos da ação são para: a) haja o esclarecimento dos novos padrões praticados pela indústria; b) tais padrões sejam objeto de um compromisso, que estejam prescritos em um código de conduta pelo qual essas regras privadas podem ser cobradas pelos órgãos públicos

e pelos próprios cidadãos e, por fim; c) haja uma auditoria dessas tecnologias por trás desses novos padrões, de modo a saber se realmente estão sendo implementados.

Ou seja, é uma nova racionalidade também de articulação da sociedade civil com o objetivo de reduzir a assimetria de informação em jogo e, ainda, que haja a formulação de um código de boa conduta pelo qual tais práticas possam ser "cobráveis".

Disso resulta, ainda, outras questões em aberto: a) será que os relatórios de impacto à proteção de dados deveriam ser públicos, como um corolário do dever de informação e transparência, tal como na arena ambiental; b) com isso, há uma sinergia para que o outro lado possa avaliar se os riscos mapeados e as ações para mitigá-los são realmente efetivas? ; c) seria desejável a participação da própria sociedade civil na formulação de códigos de boas condutas?

Há, de fato, uma nova racionalidade regulatória para esse campo específico. Na medida que isso for isso assentado, nós iremos conseguir, de certa maneira, alçar a privacidade e proteção de dados pessoais cada vez mais como um elemento de competitividade e vantagem econômica, onde esses próprios agentes econômicos irão perceber a importância disso e terão cada vez mais demanda e mercado para que terceiros como certificadoras prestem esse tipo de serviço e que realmente a tecnologia melhore e facilite a proteção de dados pelos consumidores e cidadãos.

Essa é uma agenda que vem lá de trás, aquela ideia do próprio Lessig de que o código é o código da tecnologia e não só é a lei, ou seja, que a própria tecnologia normatize condutas e que deve ser investigado qual é o seu papel para melhorar e proteger a privacidade do cidadão. É isso, por exemplo, o que é expressado pelas chamadas privacy-enhancing technologies.

E aí teremos esse enorme desafio, nova racionalidade, novo padrão, digamos assim, na arena de proteção de dados pessoais no mundo e o que fazemos disso no Brasil? Será que o Brasil está preparado para isso tudo? Será que temos capacidade institucional para ter esse tipo de fiscalização do que o setor privado faz? Que é um pouco do que gostaria de falar na última parte.

Primeiro, esse sistema, essa nova racionalidade, só funciona se você tem dentro do Estado uma agência forte de proteção de dados pessoais e esse é o grande elefante branco que temos aqui no Brasil, uma lei de proteção de dados pessoais sem ainda uma autoridade de proteção de dados pessoais, então, não conseguimos nem startar, começar essa conversa se não temos uma autoridade de proteção de dados pessoais. É essa autoridade que vai validar códigos de boa conduta, é ela que vai falar se uma certificadora é de boa reputação, é a autoridade que vai aprovar as Binding Corporate Rules, é a autoridade que vai validar essas normas privadas criadas pelos agentes econômicos.

Mas , vamos supor que daqui um tempo teremos a autoridade de proteção de dados pessoais. No Brasil, como iremos lidar com isso? Primeiro temos que olhar nosso contexto, qual é o conteúdo que vamos dar, tangibilizar, dar vida a essa regulação. Por exemplo, em termos de capacidade institucional, mesmo que se crie essa autoridade, ainda assim, precisamos olhar para essa autoridade e ver - ela tem recursos financeiros e humanos para dar conta dessa missão regulatória atribuída? Por exemplo, se você pega a Federal Trade Comission (FTC), ou mesmo a autoridade francesa de proteção de dados pessoais, o que eles criaram dentro dessas instituições foram tech labs, ou seja, não basta

apenas o cientista político, advogado, ou assim por diante, eu preciso trazer expertise dos engenheiros e dos cientistas de computação, são esses caras que irão dizer se uma tecnologia incorpora o que está na regulação. Se olhamos para alguma das maiores investigações da FTC, foram os engenheiros olhando os códigos de linha de páginas de site para ver se existia um cookie de monitoramento dos consumidores e usuários que não estava presente nas políticas de privacidades. Nós, enquanto advogados, não vamos conseguir realizar isso, então teremos que olhar se essa autoridade terá esse tipo de capacidade institucional.

Outra questão, no Brasil nós temos uma sociedade civil articulada, mas será que essa atividade civil articulada está preparada para essa pauta específica de proteção de dados pessoais? Por que estou dizendo isso? Se você vai nos EUA, você tem a Electronic Privacy Information Center/EPIC que só lida com isso, o tema da privacidade. Você vai para a Europa, a mesma coisa, como, por exemplo, com It's not your Business/NOYB especializada em privacidade e proteção de dados pessoais, será que conseguiremos criar isso no Brasil? Centros de pesquisa já vemos aparecendo, mas mais do que isso, será que teremos mídia especializada para fazer jornalismo investigativo sobre essas questões, como, por exemplo, a República vem fazendo?

Ou seja, não se trata apenas do cidadãos, agentes econômicos e também do Estado, precisamos ter todo um ecossistema articulado nisso.

Um dos pontos chaves a esse respeito é, por exemplo, pensar no Estado para além da figura do regulador, mas, também, como um grande consumidor de tecnologia. Será que na agenda de cidades inteligentes, municípios, governos, administração pública, conseguiremos fazer o mercado para ter melhores práticas? Como editais de licitação poderiam colocar privacidade e proteção de dados como um diferencial, para se criar justamente incentivos econômicos para que sejam gestadas essas tecnologias de melhoria da privacidade. Qual o papel, por exemplo, de bancos públicos como o BNDES? O BNDES tem uma linha de financiamento só de internet das coisas, será que não seria o caso de condicioná-los à programas de privacidade? Mais ou menos da seguinte forma, me mostra aqui que se o seu dispositivo tem privacy by design e então você se torna elegível para essa taxa de juros abonada. Será que a conseguimos enxergar no futuro que essa autoridade vai ter capacidade de coordenação com a ANATEL, agência nacional de saúde e tantas outras agências reguladoras que o Brasil tem, porque todos esses setores vão lidar com dados. E

E, por fim, a última questão, que penso ser a principal de todas, essa nova racionalidade regulatória foi criada e foi gestada na maioria das vezes em ambientes que já tinham um ambiente de proteção de dados pessoais, União Europeia, EUA com sua regulação setorial. No entanto, no Brasil, nós não temos essa cultura de proteção de dados pessoais, será que em quanto tempo teremos essa cultura, a qual, penso eu, vai conseguir, de certa forma, ativar todos esses mecanismos previstos na nossa lei geral de proteção de dados pessoais? Quem serão aquele acadêmico e aquele outro ativista que se juntaram para questionar qual era o código de boa conduta de uma grande indústria? Quem serão os setores que largarão na frente e compreenderão a importância de tangibilizar as metas da regulação frente às suas particularidades?

Enfim, o que eu busquei trazer aqui para vocês é que temos um diagnóstico bem claro: há uma nova racionalidade regulatória no campo de proteção de dados pessoais, mas temos uma série de desafios e perguntas a serem respondidas dentro

da particularidade do Brasil e, esse transplante, pode ou matar quem tá recebendo o transplante, ou pode, realmente, dar uma sobrevida para nós que já estamos muito atrasados nessa agenda. Muito obrigado!