"O *Marco Civil* e além: governança de privacidade para o futuro"

Por Martin Abrams

21 de setembro de 2014

Prefácio

Em 2014, o Brasil adotou o Marco Civil da Internet, Lei Nº 12.965 (à qual nos referiremos como "Marco Civil"), contendo as disposições sobre privacidade. A finalidade dessas disposições é a de proporcionar aos brasileiros o controle de seus dados quando eles estiverem on-line. Este artigo não pretende ser uma revisão dessas disposições, mas antes, uma discussão mais ampla sobre o que constitui uma governança de privacidade eficaz, prática e equilibrada. Durante a elaboração deste artigo, analisei dispositivos legais da Europa, das Américas e da região da Ásia-Pacífico, bem como o atual debate global sobre governança de privacidade eficaz. O documento reflete os meus pontos de vista, mas não é, necessariamente, o reflexo da *Information Accountability Foundation*, uma organização educacional e de pesquisas que coordeno, ou dos fundadores da Fundação.

Introdução

Nós, seres humanos, evoluímos como uma espécie social. Viajamos em grupos e nos reunimos em famílias. Somos muito curiosos a respeito de nossos vizinhos, mas procuramos não sermos vistos por eles porque também somos uma espécie que gosta de privacidade. Às vezes, almejamos a reclusão e mantemos segredos dentro dos nossos grupos sociais.

Também somos uma espécie com um senso histórico. A partir dos desenhos nas cavernas, nós sempre acumulamos reflexos dos nossos pensamentos e descrições de eventos importantes. À medida que evoluímos, nossas tecnologias para o registro de histórias também evoluíram concomitantemente. De século em século, as novas tecnologias abalaram o equilíbrio entre o nosso social e a nossa privacidade. Provavelmente, a primeira grande erupção foi o desenvolvimento da escrita na antiga Suméria. Quatro mil anos mais tarde surgia a prensa móvel e, outros quatrocentos anos depois, a máquina fotográfica Brownie que motivou o artigo de revisão da lei de Brandeis e Warren sobre privacidade[1]. Na sequência, tivemos o Rádio e a TV.

Logo após veio o computador, e a revolução das comunicações realmente decolou. A Internet tornou-se um meio de consumo em meados da década de 1990 e o iPhone foi lançado em 2007, expandindo a observação maciça para além do PC. O grande volume de dados (*big data*) começou na primeira década deste século, quando os cientistas desenvolveram técnicas que facilitaram o processamento de dados não estruturados, tal como imagens digitais como parte de analíticas avançadas. As tecnologias

[1] Brandeis, Louis e Samuel Warren (1890), "The Right to Privacy", *Harvard Law Review*, volume 4, number 5, pp. 193-220.

expandiram a natureza dos grupos – redes sociais possibilitaram novas associações espontâneas à distância, o compartilhamento de *insights* e os vínculos entre passado, presente e previsões do futuro.

Durante a Copa do Mundo de 2014, visitantes no Brasil postaram milhões de fotos pelas redes sociais, usando seu próprio dispositivo de vigilância pessoal, também conhecido como o telefone inteligente (*smart phone*). O CFTV foi uma das ferramentas usadas pela polícia para manter a ordem. Alheios ao fato de estarem sendo observados por estranhos, torcedores comemoraram as vitórias e lamentaram as derrotas com amigos e, em seguida, compartilharam suas tristezas e alegrias com confidentes por meio de fotos e postagens, com os metadados dessas expressões passando por milhares de mãos.

Em todo o país, as autoridades planejaram e se prepararam para todos e quaisquer eventos humanos que pudessem causar riscos, fazendo uso da análise de grandes dados. Essa análise será ainda mais atualizada em relação à preparação das Olimpíadas de 2016.

Este é o ambiente no qual tanto implementamos o Marco Civil quanto contemplamos um novo regime de privacidade.

Dados impulsionam a economia moderna

O conhecimento é o novo capital em uma economia e sociedade modernas, e o conhecimento está fundamentado em dados. Neil Richards e Jonathan King[2] referiram-se à nova combinação tecnológica como o grande computador de metadados e às regras que regerão essa mescla gigante de dados quanto a privacidade. Eles enxergam a privacidade como o compêndio de regras que governa a justa originação e a administração das informações que a todos nós concernem e pertencem. Faço uso da palavra "concerne" intencionalmente. Grande parte dos dados que são armazenados a nosso respeito não provém diretamente de nós. Isso será ainda mais discutido em uma seção adiante sobre taxonomias de dados. No entanto, as impressões que alguém tenha a meu respeito não são de minha propriedade, mas são de propriedade dele. Eu posso ter um interesse em como elas possam ser usadas e exigir proteções contra o seu indevido uso. Entretanto, eu não posso reivindicar a propriedade desses dados.

A finalidade deste artigo é a de explorar a aplicação do compêndio de regras em uma sociedade moderna impulsionada por dados e sua aplicabilidade tanto no Marco Civil quanto em qualquer nova lei da privacidade que possa vir a substituí-la. Especificamente, esse artigo:

- Definirá a privacidade e a proteção de dados;
- Fornecerá um histórico da lei da privacidade;
- Sugerirá uma taxonomia de dados com base na origem dos dados e a vinculará a uma política eficaz;
- Discutirá a governança de processamento com base no estabelecimento da base jurídica;
- Descreverá a responsabilização com base nas proteções da privacidade; e
- Fornecerá diversas sugestões práticas.

[2] Richards, Neil M. and Jonathan H. King (Forthcoming 2014), “Big Data Ethics”, *Wake Forest Law Review*, Wake Forest University School of Law, Winston-Salem.

Principais definições do conceito – privacidade e proteção de dados

Países com uma tradição de direito civil normalmente contam com leis de proteção de dados enquanto aqueles com tradição de direito comum possuem leis de privacidade. São elas iguais? O Grupo de Trabalho do Artigo 29 (WP29)[3], composto por todas as autoridades europeias de proteção de dados, lançou um documento na primavera de 2014 que proporcionou orientação no equilíbrio entre os interesses das companhias com os dos indivíduos durante o processamento de dados. O artigo argumentou que a proteção de dados é um conceito muito mais amplo de privacidade. Esta distinção foi mais desenvolvida em um artigo de Peter Hustinx, Supervisor de Proteção de Dados Europeus, intitulado "Lei de Proteção de Dados da UE: A Revisão da Diretiva 95/46/CE e o Regulamento Proposto de Proteção Geral de Dados"[4]. Hustinx delineia o conceito de privacidade a partir da Declaração Universal dos Direitos Humanos das Nações Unidas e da Convenção Europeia dos Direitos Humanos. Estes documentos definiram a privacidade como sendo o direito ao respeito pela sua vida privada e familiar, seu lar ou sua correspondência. De acordo com Hustinx, o Conselho da Europa considerou o conceito de privacidade como sendo muito limitado e propôs um conceito mais amplo de proteção de dados, o qual proíbe o tratamento inadequado das informações. Tanto o WP29 como Hustinx argumentam que, além disso, a proteção da privacidade dos dados facilita os direitos afetados pelas informações, tais como emprego, liberdade de expressão da família e participação econômica. Eles argumentariam ainda que a privacidade, na forma mais limitada do termo, refere-se ao respeito por esses interesses mais próximos do indivíduo, como família e lar.

Existem centenas de definições para privacidade. Eu argumentaria que a privacidade sob a Lei Canadense possui uma interpretação muito ampla, mais parecida com a proteção de dados. Para o propósito deste artigo, seria útil para o leitor ter uma noção da definição de privacidade do autor e de como ela se relaciona com a proteção de dados.

Em primeiro lugar, por privacidade quero exprimir a privacidade informacional. Também há a privacidade física que se relaciona a quando outras pessoas podem nos ver e nos ouvir. Por exemplo, uma câmera que o observa enquanto você troca de roupa é um abuso de privacidade física. Ela o está observando quando você não espera ser observado. Entretanto, quando as imagens capturadas pela câmera são digitalizadas, armazenadas e passadas para serem processadas, isto é um assunto que diz respeito à privacidade da informação. A observação de sua pessoa física—quando inesperada—é um abuso de privacidade física, enquanto o processamento da informação (imagem digital) diz respeito à privacidade informacional. O domínio deste artigo é a privacidade informacional. Quando utilizo o termo privacidade, quero referir-me à privacidade informacional.

---

[3] O Artigo 29 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho da Europa criou um Comitê chamado *Working Party 29* (Grupo de Trabalho 29), composto de todas as autoridades nacionais de proteção de dados para incentivar a harmonização das leis nacionais de acordo com a Diretiva. A Comissão fornece orientação de mercado por meio de opiniões. O Grupo de Trabalho 29 não possui nenhuma autoridade reguladora real.

[4] Hustinx, Peter (2014), "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

Em segundo lugar, por privacidade, quero referir-me à ausência do processamento inadequado de informações que dizem respeito a uma pessoa identificável. Adequado pode ser definido pelas leis, regulamentos, acordos, contratos e até por expectativas bem estabelecidas. Por exemplo, usar informações sobre o meu estado de saúde para me discriminar em termos de emprego seria uma violação de privacidade, porque a lei proíbe que essas informações sejam usadas para essa finalidade. Eu não limito a privacidade à habilidade do indivíduo de manter o controle sobre os dados ou ao direito de não ser incomodado. Essas estão entre as definições de privacidade que são mais restritas.

Proteção de dados é o sistema de regras que impede o processamento inadequado dos dados. Por exemplo, a lei europeia de proteção de dados exige que as organizações tenham uma base jurídica para efetuar qualquer processamento de dados. Ela ainda estabelece seis bases jurídicas para esse processamento. É responsabilidade do controlador de dados estabelecer a base jurídica para esse processamento.

O amplo conceito de privacidade que descrevo é muito semelhante à proteção de dados. Funcionalmente, existem algumas diferenças entre a lei da privacidade bem estabelecida em países como Nova Zelândia e Canadá, que seguem um modelo de lei comum, bem como uma lei de proteção de dados em sociedades de direito civil. De fato, é possível ver uma mistura entre a abordagem baseada nos efeitos da lei da privacidade e a natureza de base processual da lei de proteção de dados.

História do direito de privacidade

A lei da privacidade informacional data de pesquisas realizadas na década de 1960 sobre os riscos a indivíduos pelo amplo uso de computadores mainframe. A pesquisa de mais impacto foi realizada pelo Dr. Alan Westin, um professor da Universidade de Columbia. Seu livro "Privacidade e Liberdade", de 1967, estabeleceu a base para as leis que começaram a surgir na década de 1970.

Em 1978, havia bastante interesse em privacidade, particularmente em como ela poderia afetar o livre fluxo de dados além das fronteiras, para fomentar a criação, pela OCDE, de uma força-tarefa de privacidade presidida pelo juiz australiano Michael Kirby. O Grupo Kirby desenvolveu uma estrutura de privacidade que foi adotada pela OCDE em 1980. As Diretrizes de Privacidade da OCDE são a base para a maioria das leis de privacidade subsequentes. As diretrizes de privacidade foram desenvolvidas numa época em que os primeiros PCs eram apenas para os adaptadores iniciantes; a maioria dos dados era fornecida em um formulário de papel impresso; o comércio estava na transição inicial das tecnologias de bancos de dados, e a Internet nem sequer era um sonho.

As Orientações da OCDE[5] continham oito princípios para o justo processamento dos dados:

1. **Princípio de limitação da coleta**
   Deve haver limites para a coleta de dados pessoais e, quaisquer desses dados, devem ser conseguidos por meios legítimos e justos e, onde apropriado, com o conhecimento ou consentimento do sujeito dos dados.

2. **Princípio de qualidade dos dados**

[5] OECD, (1980) "OECD Guidelines on the Protection of Privacy and Transborder Data Flows", OECD, Paris.

Os dados pessoais devem ser relevantes para os propósitos aos quais devem ser utilizados e, na medida necessária para esses propósitos, eles devem ser exatos, completos e atualizados.

3. Princípio da especificação do propósito

Os propósitos para os quais os dados pessoais são coletados devem ser especificados, ao mais tardar, na época da coleta dos dados, e o uso subsequente deve ser limitado à realização desses propósitos ou a qualquer outra finalidade que seja compatível, e que sejam especificados sempre que uma alteração de propósito seja necessária.

4. Princípio de limitação de uso

Os dados pessoais não devem ser revelados, disponibilizados ou de outra forma utilizados para fins diferentes daqueles especificados em conformidade com o Parágrafo 9 (o terceiro princípio, acima), salvo com:

a) O consentimento da pessoa em causa; ou

b) Pela autoridade da lei.

5. Princípio de salvaguardas de segurança

Os dados pessoais devem ser protegidos por meio de salvaguardas razoáveis de segurança contra riscos, tais como perda ou acesso não autorizado, destruição, utilização, modificação ou revelação de dados.

6. Princípio de abertura

Deve haver uma política geral de abertura sobre os desenvolvimentos, práticas e políticas relacionados aos dados pessoais. Os meios devem estar prontamente disponíveis de forma a estabelecer a existência e a natureza dos dados pessoais e os principais propósitos de sua utilização, assim como a identidade e a residência habitual do controlador dos dados.

7. Princípio de participação individual

Um indivíduo deve ter o direito:

a) De obter de um controlador de dados ou, de outra forma, a confirmação de saber se o controlador de dados possui ou não dados a seu respeito;

b) De ser comunicado sobre os dados que lhe dizem respeito:

i) Dentro de um prazo razoável;
ii) A um custo, se houver, que não seja excessivo;
iii) De uma maneira razoável; e
iv) De uma forma que lhe seja inteligível;

c) Ser-lhe apresentado motivos, no caso de um pedido, segundo os subparágrafos (a) e (b), ser-lhe negado e ter condições de contestar essa negação; e

d) De contestar dados a ele relacionados e, se a contestação for bem sucedida, fazer com que os dados sejam apagados, corrigidos, completados ou alterados.

8. **Princípio de responsabilização**

Um controlador de dados deve ser responsável pelo cumprimento das medidas que dão efeito aos princípios acima enunciados.

Coletivamente, esses oito princípios são conhecidos como *Fair Information Practice Principles* (Princípios Justos da Prática das Informações) ou "FIPS". Embora existam outras versões de FIPS, todas procedem das Diretrizes da OCDE.

Os primeiros pensadores da privacidade enxergaram-na melhor praticada se houvesse uma cadeia de controle estabelecida. O indivíduo começa a ter controle dos dados a seu próprio respeito e, seletivamente, os cede a outros para propósitos particularmente definidos. Podemos ver isso nas diretrizes da OCDE a partir do princípio da coleta que especifica que os dados devem ser coletados, onde possível, com o consentimento do indivíduo. Este conceito de controle também é contínuo com os princípios do propósito e do uso. O conceito de consentimento expresso no Marco Civil segue diretamente esses pensamentos iniciais sobre controles de privacidade, mas vai um passo além. O consentimento adequado pode fluir diretamente de uma transação. Por exemplo, quando alguém compra móveis e pede para que eles sejam entregues em um determinado endereço, o indivíduo está insinuando que ele ou ela esteja concedendo o consentimento com que o endereço seja compartilhado com o serviço de entrega. A exigência do consentimento expresso, apresentado pelo Marco Civil, pode ser entendida como uma chamada para o consentimento explícito para todos os tipos dessas ações. Isso cria um processo que é, ao mesmo tempo, oneroso para todas as partes e dilui o efeito do consentimento explícito nos casos em que seja adequado fornecer proteção.

Conforme mencionado anteriormente, nem todos os dados que nos pertencem procedem diretamente de nós. Nós somos uma espécie muito curiosa. Observamos os outros e essas observações se tornam impressões. Ao memorizarmos essas impressões, elas se tornam dados que pertencem a outros, mas não estão sob seu (dos outros) controle. Essas observações sempre existiram na forma de notas e até de livros de contabilidade, tal como elas eram quando as Diretrizes da OCDE foram adotadas. Com o passar do tempo, as impressões se tornaram uma parcela maior dos dados totais e também se tornaram dados digitais. Hoje, as observações já não exigem os olhos, ouvidos e nariz de um indivíduo, graças às tecnologias tal como cookies ou beacons, dispositivos como sensores ou sistemas como o CFTV.

Dessa forma, a evolução tecnológica originou uma tensão entre o conceito do indivíduo como controlador do arquivo e da natureza de como os dados são originados, os quais serão explorados na seção seguinte.

Taxonomia de dados

Uma simples leitura do Marco Civil sugeriria que a lei fosse mais aplicável aos dados prontamente fornecidos pelo indivíduo ou observados pelo servidor da Internet. Para compreender as diferenças entre esses dois tipos de dados, além dos dados não explicitamente cobertos pela legislação, uma taxonomia de dados pode ser útil.

A lei da privacidade informacional é essencialmente a regulamentação do processamento de dados que dizem respeito a indivíduos de uma forma que possam ser ligados a esses mesmos indivíduos. O termo para esses dados, que são o domínio para a aplicação da lei da privacidade, são dados pessoais. Os dados sobre animais, vegetação e materiais não são o domínio para a lei da privacidade. Dados sobre indivíduos humanos por nome, endereço ou outros identificadores estão claramente dentro do domínio da lei da privacidade. Os dados que podem ser conectados de forma a serem vinculados a um único

indivíduo podem ser o domínio para a lei da privacidade. Esta última categoria, dados que podem ser conectados, foi expandida exponencialmente pelo surgimento de novas tecnologias da informação e da comunicação.

A necessidade de governar eficazmente essas novas tecnologias criou uma demanda por novas taxonomias de dados. Em março de 2014, a OCDE realizou um workshop para analisar a sua estrutura de privacidade e os desafios que possam surgir de um grande volume de dados. A *Information Accountability Foundation* preparou uma nova taxonomia baseada em como os dados são originados [6]. A seção a seguir foi extraída diretamente desse trabalho e ajuda a ilustrar os desafios que as novas tecnologias criam para os sistemas, ainda mais se os sistemas de governança contemplarem apenas o consentimento expresso.

Contexto

Observando a evolução do processamento de dados, a Fundação foi capaz de isolar quatro classificações de dados com base em sua origem. Estes antecedentes delineiam o desenvolvimento das quatro classificações: Fornecidos, Observados, Derivados e Inferidos.

Fornecidos

Em 1967, quando o livro "Privacidade e Liberdade" foi publicado, a grande maioria dos dados processados por computadores que pertenciam a indivíduos foi oriunda diretamente de ações conscientes e voluntárias do indivíduo.[7] Em uma solicitação de empréstimo, no registro de uma escritura, na abertura de uma conta, no pedido de uma licença, no pagamento de uma fatura ou em sua formatura escolar. Todas essas ações discretas criariam um registro que verdadeiramente envolveria o indivíduo. Dentro deste cenário, as ações eram comparadas com uma coleta de dados da qual o indivíduo participava. Assim, a coleta e a origem eram uma e a mesma.

Observados

Na época havia pequenos conjuntos de dados observacionais, mas a maioria não era informatizada. Os médicos criavam anotações sobre seus pacientes em históricos médicos em papel, os pequenos comerciantes faziam anotações sobre seus melhores clientes e os primeiros marqueteiros anotavam semelhanças sobre seus melhores clientes. Esses conjuntos de dados, na maioria manuais,—criados sem o envolvimento do indivíduo—eram, em grande parte, insignificantes o suficiente para afetar um modelo de governança que era, de modo geral, baseado na autonomia individual. Esta taxonomia classificará esta categoria de dados como observados.

Derivados

Assim como existiam dados que diziam respeito a um indivíduo, assim também existiram outros que buscavam semelhanças nos dados. Os comerciantes estiveram classificando seus clientes com base em atributos comuns desde que existiram compradores e vendedores. No século XIX, na América

[6] Abrams, Martin (2014), "The Origins of Personal Data and its Implications for Governance", The Information Accountability Foundation, http://informationaccountability.org/wpcontent/uploads/Data-Origins-Abrams.pdf.
[7] Alguns dos primeiros computadores modernos foram utilizados na Segunda Guerra Mundial tendo como alvo a artilharia e o desenvolvimento de armamento. Os computadores foram então usados para pesquisas científicas. O uso de computadores para processar dados relativos a pessoas, tais como dados de folha de pagamento, ocorreu posteriormente.

do Norte, os comerciantes criaram cooperativas para compartilhar informações sobre mérito de crédito com classificações derivadas de dados compartilhados. A indústria do marketing direto começou com o simples processo de utilizar os dados transacionais para obter segmentos de mercado com base nas semelhanças. Além disso, a partir do momento em que os analistas iniciaram a busca por semelhanças, eles começaram a efetuar simples cálculos matemáticos com o intuito de aprimorar as comparações. Por exemplo, poderia a proporção da dívida hipotecária em relação à dívida do consumidor demonstrar alguma coisa interessante? Os produtos destes cálculos simples são dados derivados de dados subjacentes. Durante anos, a indústria de seguros observou o nascimento, morte, ocupações, localização e estilo de vida, e derivaram tabelas atuariais que ainda são usadas para a subscrição em um seguro de vida. Embora a classificação se baseia em dados que decorrem de interações e transações que envolvem o indivíduo, o próprio indivíduo não está envolvido na criação dos novos dados. A taxonomia classificará esses dados como derivados.

Inferidos

Uma aplicação inicial da estatística informatizada em relação aos grandes conjuntos de dados pessoais foi a pontuação de falências, desenvolvida pelo MDS e Fair Issacs na década de 1980. A pontuação fez uso dos relatórios de crédito informatizados para prever a probabilidade de um indivíduo poder falir nos próximos cinco anos. A pontuação de crédito do MDS não era apenas uma correspondência dos atributos dos indivíduos que faliram, mas, ao contrário, era uma previsão de base estatística que era validada pelo uso de dados históricos. O resultado da pontuação de crédito é uma parte dos dados baseados na probabilidade da ocorrência de um evento futuro ligado a um indivíduo. Embora os dados subjacentes resultassem de interações com o indivíduo, o próprio indivíduo não teve qualquer envolvimento na criação da pontuação. A classificação para esses dados é inferida.

Os dados se expandiram rapidamente desde a invenção dos computadores modernos, durante a Segunda Guerra Mundial. A rápida mudança das tecnologias da informação e da comunicação levou à expansão de conjuntos de dados ao final das décadas de 1980 e 1990. O fator de desencadeamento mais significativo para a expansão dos dados foi a explosão literal de dados observacionais que foi provocada pela Internet, na década de 1990. O século XXI trouxe as tecnologias dos sensores que possibilitam a observação granular nos mundos físico e virtual. A combinação da observação física e on-line tem facilitado a expansão maciça de dados observacionais. Embora esses dados comecem com as ações dos indivíduos, os próprios indivíduos não são parceiros ativos na própria originação dos mesmos. Durante a última década, os cientistas aprenderam como utilizar dados não estruturados em modelos analíticos que preveem o comportamento futuro. Isso expandiu significativamente o volume de dados que poderiam ser utilizados para a pesquisa, pois os dados não precisavam mais ser formatados em campos tradicionais. Com base na probabilidade, a Informática tem cada vez mais capacidade de colocar os indivíduos em ordem de classificação, o que levou a uma expansão rápida de dados inferidos.

<u>Taxonomia com base na origem</u>

A nossa taxonomia com base na origem estabeleceu quatro classificações para dados baseadas em como os dados são originados:

1. **Fornecidos**

Os dados fornecidos são originados por meio de ações diretas adotadas pelo indivíduo das quais ele ou ela está plenamente consciente das ações que levaram à originação dos dados. Os dados fornecidos incluem registros, solicitações de pesquisas e qualquer instância na qual o indivíduo venha a fornecer dados com completa consciência de que ele ou ela assim o esteja fazendo.

2. Observados

Dados observados são simplesmente o que é observado e registrado. O surgimento da Internet como meio interativo do consumidor tornou possível observar e digitalizar dados de uma forma mais robusta. Na Internet é possível observar de onde o indivíduo veio, o site que ele ou ela está visitando, quantas vezes ele ou ela o observa e até mesmo a duração das pausas. O reconhecimento facial e a Internet das coisas estão tornando possível a observação de uma maneira digital no mundo físico.

3. Derivados

Os dados derivados são aqueles que simplesmente derivam de uma maneira bastante mecânica de outros dados e se tornam um novo elemento de dados relacionado ao indivíduo. Por exemplo, as razões simples calculadas a partir de outros dados, são dados derivados. Os agrupamentos de marketing também são um exemplo de dados derivados.

4. Inferidos

Os dados inferidos são o produto de um processo analítico baseado em probabilidade. As pontuações de crédito e de identidade são exemplos, como também são muitas as inferências que resultam da análise de grandes dados.

A tabela a seguir estabelece as classificações de dados de forma mais detalha. A coluna 1 enumera as principais classificações com base em como os dados são originados. A coluna 2 contém as subclassificações que ajudam a tornar a análise mais granular. Por exemplo, alguns níveis de observação são antecipados, a subclassificação ativa, enquanto outros são alheios ao indivíduo, tais como a subcategoria passiva. A coluna 3 inclui exemplos para auxiliar o leitor a relacionar as categorias ao mundo dos dados. A coluna 4 fornece uma simples classificação do quanto o indivíduo típico pode estar consciente com base na distância e na forma da originação dos dados. A governança de dados legados, a maioria das leis se baseia nas Diretrizes da OCDE e na Diretiva da UE, é muito dependente da consciência individual para exercer o consentimento bem como a revisão dos dados (direitos de acesso) e a correção.

Tabela 1: Categorias de dados com base na origem

Categoria	Subcategoria	Exemplo	Nível de consciência
Fornecidos	Iniciado	○ Solicitações ○ Registros ○ Registros públicos, tais como licenças ○ Compras com cartão de crédito ○ Histórico médico, conforme fornecido pelo indivíduo	Alto
	Transacional	○ Pesquisas respondidas ○ Pressão arterial ou peso, conforme registrado no prontuário de atendimento	Alto
	Postado	○ Discursos em ambientes públicos ○ Postagens na rede social ○ Serviços de fotografia ○ Sites de vídeo	Alto
Observados	Noivo/a	○ Cookies em um site ○ Cartão fidelidade ○ Sensores de localização habilitados em dispositivos pessoais	Médio
	Não Antecipado	○ Fitness em trilhas usando dispositivo portátil ○ Tempo de pausa sobre um pixel na tela de um tablet	Baixo
	Passivo	○ Imagens faciais do CFTV ○ Tecnologias obscurecidas da web ○ Leitores Wi-Fi em edifícios que estabelecem a localização	Baixo
Derivados	Computacional	○ Razões de crédito ○ Média de compra por visita ○ Risco de desenvolver uma doença com base em uma única	De Médio a Baixo
	Notacional	○ Classificação baseada em atributos comuns de compradores ○ Problema médico baseado em testes de	De Médio a Baixo
Inferidos	Estatístico	○ Pontuação de crédito ○ Pontuação de resposta	Baixo
	Analítico avançado	○ Risco de desenvolver uma doença com base em uma análise de múltiplos fatores ○ Pontuação de sucesso na faculdade com base na análise de grandes dados	Baixo

Análise da taxonomia

O Marco Civil utiliza o consentimento expresso como meio de governar dados originados por meio da Internet. A questão inicial que devemos perguntar é se o consentimento é um meio viável para a governança da privacidade na Internet. A segunda pergunta é se este é o melhor mecanismo. Entretanto, a terceira pergunta estaria relacionada com a privacidade no Brasil, além da Internet.

Muitos desses dados pessoais da Internet são fornecidos diretamente pelo indivíduo por meio de inscrições, comentários e interações com o navegador que são claramente participativos. Dados adicionais são originados por meio da observação das ações do indivíduo enquanto ele está on-line. Por exemplo, a período de tempo no qual um consumidor faz uma pausa sobre um pixel pode ser um ponto de dados, mas ele é mais observado do que fornecido. Além disso, mais dados são inferidos por meio da modelagem dos dados fornecidos e observados. Alguns dos dados inferidos são utilizados para a comercialização, para fins de faturamento ou para determinar qual parte de um site está sendo usada ou não, enquanto outras inferências são usadas para proteger os servidores e também a rede.

O consentimento é um meio viável de governança na Internet, uma vez que existem oportunidades para que as pessoas leiam um aviso e concedam o consentimento com base no aviso. Mas, quão eficaz é esse consentimento quando vamos além dos dados fornecidos para os dados observados? Será que o indivíduo transferirá o conhecimento adquirido pelo aviso para uma percepção da coleta passiva que ocorre por meio da observação?

Alguns argumentariam que o consentimento expresso, tal como é previsto na lei, amplia as proteções. No entanto, o consentimento expresso é apenas tão robusto quanto o entendimento do indivíduo em relação ao aviso de especificação do propósito subjacente. À medida que os usos se tornam mais complexos, é provável que o entendimento diminua. Além disso, à medida que os usos se tornam mais complexos, o consentimento expresso exigiria mais consentimentos dos indivíduos. A fadiga ocasionada pelos consentimentos torna-se um problema e, dessa forma, os consentimentos logo são agrupados. Nesse ponto, eles se tornam menos significativos. Malcolm Crompton, antigo Comissário da Privacidade Australiana, tem argumentado que o consentimento torna-se, então, uma transferência do risco da corporação que utiliza os dados para o indivíduo que está assumindo o risco ao conceder um consentimento.

À medida que nos afastamos da natureza interativa da Internet para o mundo em geral, os desafios para o consentimento tornam-se até maiores. Ao considerarmos os 3000 sensores existentes em um carro novo monitorando o seu desempenho, assim como o desempenho do motorista, podemos começar a enxergar o desafio para a governança do consentimento. E o carro é apenas um exemplo de um mundo totalmente ligado em rede, onde os sensores são incorporados nos produtos que utilizamos no dia a dia. Acrescentam-se as câmeras de CFTV utilizadas para proteger a segurança pública e, dessa forma, poderemos ver mais outros tantos desafios.

Os comentários acima não têm a intenção de subestimar o valor e a finalidade do consentimento. Onde o consentimento é eficaz, este deve ser o principal mecanismo de governança. O consentimento funciona bem quando o indivíduo é o provedor ativo dos dados. Entretanto, até nas circunstâncias

onde o consentimento funciona, ele não é uma salvaguarda em si mesmo. A proteção da privacidade é dependente da administração dos dados na medida em que nos afastemos do processo no qual os indivíduos são os provedores de dados e, portanto, são eles que estão, na realidade, sob controle.

Base jurídica relacionada ao processamento

Algumas leis de proteção de dados legados relacionadas aos casos nos quais o consentimento não é eficaz para a proteção de indivíduos. A Diretiva Europeia de Proteção de Dados (Diretiva 95/46/EC)[8] estabelece a governança na base jurídica de uma organização para processar dados pessoais. Apesar do método preferido contido na Diretiva, o consentimento é uma das seis bases jurídicas. O Artigo 7 prevê:

> Os Estados-Membros deverão determinar que os dados pessoais somente poderão ser processados quando:
> (a) A pessoa dos dados em questão tenha concedido o seu consentimento de forma inequívoca;
> (b) O processamento é necessário para a execução de um contrato no qual a pessoa dos dados é uma das partes ou a fim de tomar as medidas solicitadas pela pessoa dos dados antes de começar um contrato.
> (c) O processamento é necessário para o cumprimento de uma obrigação legal à qual o controlador está sujeito; ou
> (d) O processamento é necessário para proteger os interesses vitais da pessoa dos dados; ou
> (e) O processamento é necessário para o desempenho de uma tarefa de interesse público, ou no exercício de autoridade oficial investida no controlador ou em um terceiro para quem os dados são revelados; ou
> (f) O processamento é necessário para os propósitos de interesses legítimos empenhados pelo controlador, ou por terceiros ou pelas partes, para quem os dados são revelados, salvo quando os interesses são prevalecidos pelos interesses dos direitos e liberdades fundamentais do sujeito dos dados, o que requer proteção segundo o Artigo 1(1.) (Que abrange os objetivos da Diretiva).

Houve mais atenção aplicada nas cinco bases jurídicas, além do consentimento, em vista de a Europa ter debatido o novo regulamento proposto para substituir a Diretiva. De interesse particular tem sido os interesses legítimos, Artigo 7, seção (f). O interesse legítimo não foi muito utilizado no sul da Europa[9]. Entretanto, o crescimento da Internet e o surgimento da Internet das coisas, o Cloud e os grandes dados fizeram com que o WP29 revisse a utilização dos interesses legítimos conforme uma base jurídica. Na primavera de 2014, o WP29 emitiu um parecer sobre a utilização do interesse legítimo, buscando comentários sobre a orientação do projeto. O parecer disse que a base jurídica correta deve ser

[8] European Parliament (1995), "Directive 95/46/EC of the European Parliament and of the Council", *Official Journal*, European Parliament, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[9] Muitas leis de proteção de dados da América Latina se baseiam nas leis do sul da Europa, principalmente na lei espanhola, mas também na lei italiana.

utilizadas com base na natureza do processamento. Por exemplo, o WP29 achou que a base jurídica adequada para processamento de dados para prevenir fraudes deve ser de interesses legítimos e não de consentimento.

Os requisitos para utilizar o interesse legítimo são muito robustos. É preciso realizar uma análise de equilíbrio de interesses. A análise deve levar em consideração os interesses legítimos do controlador e todos os interesses dos indivíduos afetados pelo processamento. Dessa forma, o controlador deve estar pronto para demonstrar o processo a um comissário de proteção de dados, quando solicitado. Os recursos para a realização dessa análise resultam de um programa abrangente de privacidade.

Responsabilização e programas abrangentes

Há uma consciência crescente de que as proteções eficazes da privacidade exigem que os controladores de dados sejam intendentes responsáveis dos dados que processam. Essa intendência de dados precisa estar fundamentada em critérios externos reconhecidos, tais como leis, regulamentos ou diretrizes. Este conceito de intendência de dados procede diretamente das Diretrizes da OCDE. Quando baseadas nos padrões da indústria, as Diretrizes podem ser referidas como uma autorregulamentação. Há um consenso crescente de que essa autorregulamentação deva ser vinculativa para as organizações por meio da executoriedade pelos órgãos reguladores. Nos Estados Unidos, muitos códigos de indústria e até mesmo o EU/U.S. Safe Harbor exige que uma organização anuncie a sua participação, para que a Comissão Federal do Comércio dos EUA possa agir contra um descumprimento como ato desleal.

Princípio 8 da responsabilização da OCDE prevê: Um controlador de dados deve ser responsável pelo cumprimento das medidas que dão efeito aos princípios acima enunciados. Para a maior parte dos trinta e quatro anos de história das Diretrizes de Privacidade da OCDE, o princípio de responsabilização ficou assentado, inativo. A lei da privacidade do setor privado canadense (PIPEDA) contém um conjunto de princípios, sendo que o primeiro é o da Responsabilização. A Estrutura de privacidade APEC contém o princípio 9 sobre a responsabilização. Como o processamento de dados se tornou mais complexo e mais dados são originados à distância pelo indivíduo, houve mais discussão sobre a criação de uma orientação com o intuito de proporcionar algum direcionamento relacionado à responsabilização. Em 2009, o Diálogo da Responsabilização Global foi criado como uma colaboração pelas diversas partes envolvidas. O “Ano Um” ocorreu em Dublin, contando com o Comissário de Proteção de Dados Irlandês como facilitador. O relatório do diálogo para o Ano Um continha os elementos essenciais da responsabilização:

- Compromisso organizacional para com a responsabilização, bem como a adoção de políticas internas consistentes com os critérios externos;
- Mecanismos para colocar as políticas da privacidade em vigor;
- Sistemas de fiscalização interna e em andamento, além de revisões asseguradas e verificação externa;
- Transparência e mecanismos para a participação individual; e
- Meios para remediação e aplicação externa.

Os elementos essenciais são o resumo para um programa de privacidade que tem a capacidade de impulsionar a utilização responsável dos dados relativos aos indivíduos. Os Reguladores Canadenses conduziram isso um passo adiante por meio da emissão da "Getting Accountability Right with a

Privacy Management Program"[10] (Obtenção de uma responsabilização correta com um programa de gerenciamento da privacidade). A orientação é dividida em duas partes. A primeira parte contém os elementos estruturais necessários para desenvolver um programa de privacidade, enquanto a parte B discute como manter e melhorar esse programa. A presença desse programa é exequível sob o princípio de Responsabilização contido nas leis.

O Comissário da privacidade de Hong Kong emitiu uma orientação semelhante em 2014. A orientação de Hong Kong é uma forte sugestão e não é exequível nos termos da lei de Hong Kong.

Os conceitos de responsabilização e os incentivos para desenvolver programas de responsabilização também estão presentes em leis de privacidade na Colômbia e no México. A Responsabilização é explicitamente parte da proposta de regulamentação da UE que, se promulgada, substituirá a Diretiva.

A Comissão Federal de Comércio dos Estados Unidos também exigiu programas abrangentes como parte dos decretos de consentimento que eles utilizam com o objetivo de resolver a aplicação.

Conclusão e recomendações

A lei da privacidade é difícil de se propor e difícil de se aplicar, pois, nós, como indivíduos, temos expectativas conflitantes. O nosso ego social quer reconhecimento e é muito curioso a respeito dos outros, enquanto o nosso ego privado quer ser protegido da visão dos outros. Por exemplo, queremos a personalização que acompanha a observação na Internet e, no entanto, não queremos ser observados. Encontrar um equilíbrio entre o nosso social e o nosso privado é muito difícil e, muitas vezes, baseia-se no contexto da interação. Isto é ainda mais exacerbado pelo ritmo da mudança nas tecnologias da informação e da comunicação. Levou quatro mil anos para passar da escrita para a prensa móvel, mas levou menos do que sessenta anos para passar dos computadores de mainframe para os telefones celulares com mais poder de computação do que os velhos mainframes. A natureza dos dados também mudou. Em 1967, quando o livro "Privacidade e Liberdade" foi publicado, a maioria dos dados foi fornecido pelo indivíduo de uma forma que o indivíduo realmente entendia. Hoje, os dados observacionais e inferidos sobrepujam os dados que fornecemos. Isso altera a equação básica da governança. Embora a governança, por meio do consentimento individual, foi muito eficaz em 1972 (quando foram promulgadas as primeiras leis de privacidade), o consentimento é muito menos eficaz— e, às vezes, ele nem sequer é viável, em governar as aplicações impulsionadas pelos dados observados e inferidos.

As economias modernas são impulsionadas pela informação da mesma forma que as economias, no século passado, foram impulsionadas pelo aço e pelas grandes máquinas. A política de privacidade deve funcionar com a política industrial de forma a criar um ambiente bem-sucedido para as pessoas. O risco à privacidade e o risco à reserva que impedem o bom uso dos dados são perigosos.

Minhas sugestões são as seguintes:

[10] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of British Colombia (2012), “Getting Accountability Right with a Privacy Management Program”, Office of the Privacy Commissioner of Canada, Ottawa, https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp.

(a) Os legisladores, quer sejam do Brasil ou de outras jurisdições, devem começar com metas bem articuladas para o teste e legislação de privacidade a fim de assegurar que a legislação realmente atingirá os objetivos. Além disso, o processo legislativo deve reconhecer que a privacidade é uma de uma série de direitos individuais que devem ser respeitados. Esses direitos incluem um amplo compartilhamento dos frutos tecnológicos. A privacidade e a inovação devem andar juntas.

(b) As leis de privacidade devem se basear em princípios, bem como devem ser tecnologicamente neutras, e especificar os resultados em vez de especificar os detalhes sobre como esses resultados podem ser alcançados. Os mecanismos mudarão assim como a tecnologia continua evoluindo.

(c) A segurança de dados não deve ser assumida. Entretanto, a lei deve exigir níveis de segurança que sejam proporcionais aos riscos dos indivíduos. A lei não deve estipular como as organizações cumprirão as especificações. As ameaças ao risco da segurança mudam com o passar do tempo e a segurança se torna uma jornada. A lei não pode antecipar o caminho da jornada.

(d) A governança não deve depender de uma única base jurídica para processar, tal como o consentimento, mas, preferivelmente, um conjunto completo de ferramentas de base jurídica, tais como assegurar os amplos interesses relacionados à vida e a felicidade do indivíduo, bem como os interesses de uma organização. Os parâmetros de equilíbrio devem ser explicados na lei, mas os mecanismos para fazer isso devem ser deixados para um processo de regulamentação. O consentimento é uma base jurídica importante e deve ser o instrumento que rege onde ele é eficaz. No entanto, o consentimento é uma das muitas bases jurídicas e não deve ser forçado onde não for eficaz.

(e) Os indivíduos têm o direito de entender como os dados que lhes pertencem serão usados. Este interesse vai muito além do conhecimento que poderia resultar de um aviso de especificação do propósito.

    i. Portanto, a transparência sobre como os dados são utilizados e os programas das organizações devem ser uma exigência por lei.
    ii. Além disso, deve ser exigido que as companhias proporcionem aos indivíduos acesso aos dados que lhes pertencem sujeito a procedimentos razoáveis para autenticação e proteção de dados que possam ser utilizados para cometer fraude.
    iii. Existem dados que não deveriam estar sujeitos a acesso. Por exemplo, dados que intencionalmente tiveram qualquer ligação com dados removidos do indivíduo não devem estar sujeitos a acesso, porque, então, isso seria uma remoção das proteções associadas com a desidentificação.[11]

(f) A lei deve exigir programas de privacidade abrangentes proporcional à complexidade organizacional. Há excelentes descrições de programas abrangentes nos materiais

[11] A desidentificação é uma metodologia que remove os identificadores de um conjunto de dados e é substituída com um código. A desidentificação geralmente é utilizada em pesquisas nas quais os dados são correspondidos por uma das partes, mas a pesquisa é realizada por outra parte. A primeira parte, que realiza a correspondência, pode ser capaz de fornecer acesso a dados. Entretanto, os pesquisadores que utilizam os dados não devem ter os meios para re-identificá-los. Se eles tivessem a ligação também teriam os meios para agir contra indivíduos. Sem as ligações, eles podem descobrir tendências sem saber quem são as pessoas. Fornecer os meios para fazê-las anularia as proteções contra a desidentificação.

fornecidos pelo projeto de responsabilização global e por agências de execução no Canadá e em Hong Kong. Os requisitos devem ser escaláveis para organizações de todos os portes e complexidades. Para facilitar a escalabilidade, as associações industriais devem ser encorajadas a desenvolver programas de melhores práticas que seriam revisados por agências executivas, podendo vir a ser adotados pelas empresas do setor. A lei espanhola de proteção de dados permite que a agência de execução reduza as multas se uma organização for capaz de demonstrar um programa abrangente. Tais incentivos devem ser considerados.

(g) A lei deve autorizar as agências reguladoras a solicitar que as organizações demonstrem seus programas, mas não deve haver uma exigência geral para que todas as companhias tenham seus programas aprovados.

(h) As agências reguladoras devem ter os recursos para monitorar o mercado, desenvolver orientações e criar um alto nível de certeza de que as organizações não conformes sejam apanhadas.

(i) O registro de dados não atendeu a qualquer propósito e, portanto, deve ser evitado em qualquer lei da privacidade.
O registro de dados foi originalmente idealizado como um meio para os indivíduos descobrirem quais as companhias que processam dados. Agora, cada companhia é um processador e essa lista não tem nenhum valor.[12]

Uma observação final, a lei da privacidade é orientada por valores humanos. Esses valores têm sido uma constante durante a história registrada. Entretanto, a tecnologia realmente afeta os mecanismos que fazem com que os valores funcionem. A lei da privacidade deve reconhecer os valores deixando, ao mesmo tempo, espaço para orientação à medida que os mecanismos se alteram com o passar do tempo.

[12] O registro de dados foi uma exigência de muitas das leis iniciais de proteção de dados. O registro de dados requer que todos os controladores registrem os bancos de dados junto às autoridades de proteção de dados. Na década de 1970, quando os primeiros requisitos apareceram, a ideia era que os bancos de dados fossem poucos e que, olhando para o registro, os indivíduos verificariam os nomes das companhias com bancos de dados. Não há qualquer registro de indivíduos realmente fazer isso em décadas. O regulamento proposto na Europa seria o de eliminar o registro.