Panorama setorial da Internet

Número 2
Junho, 2019
Ano 11

Privacidade e dados pessoais

Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação[1]

Por Laura Schertel Mendes[2]

A coleta, o processamento e a utilização de informações de caráter pessoal em enormes quantidades são componentes inequívocos da sociedade contemporânea. O interesse do Estado e também de entes privados por esse tipo de informação decorre do múltiplo proveito que pode ser tirado do processamento de dados: da publicidade direcionada a produtos personalizados, da vinculação de clientes a avaliações de risco. Quando consideramos o ambiente digital, este quadro fica ainda mais impressionante, tendo em vista que muitos modelos de negócio na Internet têm como fundamento central o processamento de dados pessoais, permitindo o financiamento de diversos serviços a partir da monetização desses dados.

Do ponto de vista do indivíduo, o conceito de "ubiquidade no processamento de dados" (*ubiquitous computing*; Mattern, 2008) parece ser ainda mais significativo ao indicar como todos os âmbitos da vida estão marcados pelo tratamento de dados pessoais. Isso se dá em razão dos inúmeros equipamentos eletrônicos que fazem parte do nosso dia a dia e que armazenam todo tipo de informação pessoal de maneira ininterrupta. Assim, além das oportunidades possibilitadas por um cotidiano informatizado e interconectado – a ampliação das formas de comunicação pessoal e pública, de mobilização social e de circulação de conhecimento, entre outras –, surgem riscos para o indivíduo, como monitoramento e vigilância crescentes, discriminação, exposição indesejada ou formação de abrangentes perfis de personalidade (Hartmann & Wimmer, 2011).

Neste contexto, atualmente a legislação sobre proteção de dados, entendida como o marco jurídico para a proteção individual em relação ao tratamento de dados e informações pessoais por terceiros, encontra-se no centro da discussão econômica, social e política em todo o mundo.

O intenso processamento de dados pelos setores público e privado a partir da década de 1970 ensejou a evolução do direito à privacidade, abarcando uma dimensão de proteção de dados pessoais, com destaque para o controle do indivíduo sobre o fluxo de suas informações na sociedade. Já a geração de normas de proteção de dados que começa a se desenvolver agora é amparada no princípio da *accountability*. Entende-se que a efetividade da proteção de dados não decorre apenas da ampliação do controle do indivíduo, mas inclui também a atribuição de responsabilidade a toda a cadeia de

[1] O presente texto tem como ponto de partida a pesquisa realizada no livro Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental (Mendes, 2014) e busca atualizar à luz da recém-aprovada Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) o modelo de proteção de dados ali proposto.

[2] Professora adjunta de Direito Civil da Universidade de Brasília (UnB) e professora do mestrado acadêmico em Direito Constitucional do Instituto Brasiliense de Direito Público (IDP). É doutora em Direito Privado pela Universidade Humboldt de Berlim.

Laura Schertel Mendes
Universidade de Brasília (UnB) e Instituto Brasiliense de Direito Público (IDP).

agentes de tratamento de dados pelos riscos do processamento de informações, uma vez que esses agentes têm mais condições de implementar medidas técnicas e organizativas capazes de proteger os dados pessoais dos titulares. Dessa forma, as legislações mais recentes, entre as quais se destaca o Regulamento Geral sobre a Proteção de Dados europeu, passam a prever novos mecanismos como relatórios de impacto, códigos de boas condutas, certificações e programas de governança, além de normas que incentivam a implementação do conceito de *Privacy by Design* (privacidade na concepção; Bennett & Raab, 2018).

A Lei Geral de Proteção de Dados Pessoais no Brasil

Até a edição da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018, o Brasil não dispunha de uma regulamentação geral sobre o tema. Diversas leis setoriais[3] formavam uma verdadeira "colcha de retalhos normativa", o que suscitava inúmeras críticas, seja pela fragilidade da proteção do titular de dados pessoais, seja pela insegurança jurídica à qual ficavam submetidas as empresas que tinham o tratamento de dados como um dos pilares de seu negócio.

Nesse sentido, há tempos se manifestavam na academia brasileira (Mendes & Doneda, 2016; Bioni, 2014) e em diferentes setores (Manifesto, 2018) vozes de defesa à edição de uma lei geral, apta a formar um sistema coerente de regras e parâmetros mínimos para o tratamento de dados no país. Assim, a aprovação da LGPD pode ser vista, em parte, como resultado do reconhecimento interno da academia e dos *stakeholders* nacionais. Além disso, fatores externos contribuíram de forma decisiva para o processo de aprovação da legislação, como a entrada em vigor do Regulamento Geral sobre a Proteção de Dados na Europa, em 2018, e os acontecimentos relacionados à empresa Cambridge Analytica a respeito da utilização de dados do Facebook para *microtargeting* na campanha eleitoral estadunidense de 2016, em violação às normas de proteção de dados[4].

A sanção da LGPD no Brasil instituiu de forma inédita no país um regime geral de proteção de dados, consolidando e complementando o marco normativo da sociedade da informação. A lei brasileira inaugura um modelo *ex-ante* de proteção de dados, fundado na ideia de que, diante do processamento automatizado e generalizado de dados na sociedade da informação, não existem mais dados irrelevantes. Uma vez que os dados pessoais são um meio de representação da pessoa na sociedade, qualquer tratamento de dados pode afetar a sua personalidade e, portanto, tem o potencial de violar seus direitos fundamentais. Essa é a razão pela qual o amparo jurídico dos dados pessoais nos moldes da LGPD realiza-se de maneira horizontal, aplicando-se a todos os setores econômicos e também ao setor público.

Por a LGPD se basear em um conceito amplo de dado pessoal, a princípio todo tratamento de dados – realizado tanto pelo setor público quanto pelo privado – está submetido a ela. Seu âmbito de aplicação abrange também a Internet. As exceções são justificadas de forma particular, seja pelo respaldo em um direito fundamental (por exemplo, a liberdade de informação, no caso da exceção

[3] Ao longo da evolução das normas de proteção de dados pessoais no Brasil, diversos documentos contemplaram o tema, como o Código Civil (Lei n. 10.406/2002), a Lei do Cadastro Positivo (Lei n. 12.414/2011), a Lei de Acesso à Informação (Lei n. 12.527/2011) e o Marco Civil da Internet (Lei n. 12.965/2014).

[4] A penalidade aplicada aos envolvidos pela Autoridade de Proteção de Dados do Reino Unido está disponível para consulta em: ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf.

à atividade jornalística) ou no interesse público relevante (como nas exceções à segurança pública e defesa nacional).

Outra inovação na lei é a ideia de que o tratamento de dados deve se amparar em uma base legal. Essas bases são variadas, destacando-se o consentimento, a execução de um contrato, o dever legal do controlador, o tratamento pela administração pública e o legítimo interesse. A seguir, examinaremos cada um desses níveis em detalhes.

Condições de legitimidade para o tratamento de dados pessoais

Um dos pressupostos fundamentais da LGPD é que o tratamento de dados só poderá ser realizado se existir uma base normativa que o autorize. Somente será legítimo o tratamento que se enquadre em ao menos uma de onze hipóteses, como o consentimento do próprio titular. Para que o consentimento seja considerado válido, ele deve ser livre, informado, inequívoco e com uma finalidade determinada.

Outra hipótese autorizativa de destaque é o tratamento de dados para o cumprimento de uma obrigação prevista em lei, em um regulamento ou para a execução de um contrato do qual o titular é parte, seja quando o tratamento for necessário para a execução de uma política pública, seja no exercício geral de suas competências ou no cumprimento de suas atribuições legais.

Quando as informações pessoais forem fundamentais para a execução de um contrato, sua coleta ou processamento estarão autorizados. É necessário a uma empresa do ramo de comércio eletrônico, por exemplo, obter os dados do cartão de crédito e do endereço do consumidor para a efetuação do pagamento e a entrega do produto, caso contrário não é possível cumprir com o contrato de compra e venda acordado.

No que se refere ao tratamento de dados pessoais para a realização de interesses legítimos do controlador ou de terceiro, deve-se sempre considerar a proporcionalidade entre esses interesses e os direitos do titular. Se a realização de uma determinada finalidade com o tratamento de dados pessoais tiver o potencial de afetar os direitos e as liberdades fundamentais do titular, tal legítimo interesse não será considerado como uma hipótese que autoriza o tratamento.

Para avaliar as condições de legitimidade do tratamento de dados, deve-se levar em conta também se os princípios da LGPD estão sendo seguidos, como os de livre acesso, segurança, transparência e qualidade. A lei procura abordar aspectos contemporâneos da proteção de dados e refletir novas demandas. Exemplos disso são o princípio da não discriminação pelo tratamento de dados, que aborda o potencial discriminatório do uso de dados ou de mecanismos de decisão automatizada que se utilizam de dados pessoais, e o princípio da prevenção, que se apresenta como a base para o desenvolvimento de medidas relacionadas à privacidade na concepção.

Outro destaque é o princípio da finalidade, que vincula o tratamento de dados pessoais ao objetivo que motivou e justificou a sua coleta. A aplicação desse poderoso princípio visa garantir a privacidade contextual, evitando que os dados sejam utilizados posteriormente para finalidades incompatíveis com aquela que primeiro permitiu sua coleta. A LGPD faz ainda uma referência expressa ao princípio da boa-fé, de fundamental importância no que se refere à proteção de dados pessoais, principalmente diante do caráter massificado de diversos mecanismos

Para que o consentimento seja considerado válido, ele deve ser livre, informado, inequívoco e com uma finalidade determinada.

(...) o titular deve ter livre acesso aos seus dados; deve poder corrigir dados equivocados e desatualizados; e deve poder cancelar dados que foram indevidamente armazenados ou cujo consentimento foi revogado por ele.

de tratamento de dados e da opacidade intrínseca a estas operações. Tal princípio orienta de forma ampla as relações entre titulares e agentes de tratamento, seja quando deveres como a transparência já estão minimamente delineados, seja quando é preciso qualificá-los.

Procedimentos para garantir a proteção de dados pessoais

Para além das condições de legitimidade, a LGPD prevê uma série de procedimentos que buscam proporcionar mais segurança e reforçar as garantias dos titulares dos dados.

Os direitos básicos atribuídos ao titular pelas diversas legislações nacionais e tratados internacionais para o controle do fluxo de seus dados são conhecidos pela sigla "ARCO", abreviação de: acesso, retificação, cancelamento e oposição. À luz do paradigma do controle, entende-se que o titular deve ter livre acesso aos seus dados; deve poder corrigir dados equivocados e desatualizados; e deve poder cancelar dados que foram indevidamente armazenados ou cujo consentimento foi revogado por ele[5]. Outros direitos relevantes são aqueles atribuídos ao titular em relação a decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, como aquelas destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito.

Nessa segunda fase do modelo de aplicação da lei, cabe aos agentes de tratamento observar, além dos direitos previstos na LGPD, as obrigações estabelecidas para todos aqueles que realizam o tratamento de dados. Entre elas, destaca-se uma obrigação a ser cumprida pelo controlador, e não pelo operador: a instituição de um encarregado pelo tratamento de dados. Tal encarregado terá como funções receber reclamações dos titulares, comunicar-se com a autoridade nacional e orientar os funcionários para que a organização cumpra com as normas de proteção de dados.

Outra importante obrigação, até então inexistente no nosso ordenamento de maneira tão abrangente, diz respeito à manutenção do registro pelos agentes de tratamento: "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (Lei n. 13.709/2018). A LGPD ainda estabelece a controladores e operadores uma obrigação central de adoção das medidas de segurança técnicas e administrativas adequadas para proteger os dados de acessos não autorizados, de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação ou de qualquer forma de tratamento inadequado.

O capítulo de segurança da informação é um pilar fundamental da LGPD e traz pelo menos três inovações importantes para o ordenamento jurídico brasileiro quanto às obrigações dos agentes de tratamento. Em primeiro lugar, a lei exige que eles adotem medidas que garantam a integridade, a confidencialidade e a dis-

[5] Os direitos do titular estão estabelecidos principalmente no art. 18 da LGPD: "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei". Disponível em: www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

ponibilidade dos dados sob tratamento. Em segundo lugar, em caso de incidente de segurança, como o vazamento de dados, o controlador é obrigado a comunicar a autoridade de proteção de dados, que pode determinar a adoção de medidas de mitigação ou a ampla divulgação para a sociedade. Em terceiro lugar, há uma obrigação que se enquadra no conceito de *Privacy by Design*, já que tais medidas deverão ser observadas desde a fase de concepção até a execução do produto ou serviço.

Fiscalização, aplicação de sanções e reparação

A terceira fase do modelo de proteção de dados consiste na responsabilidade dos agentes na hipótese de ocorrência de danos decorrentes do tratamento de dados. Na LGPD, essa responsabilidade é estabelecida tanto na forma civil quanto na forma administrativa.

A consideração da responsabilidade civil dos agentes leva em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, limitada pela LGPD às hipóteses que possuem fundamento legal, que englobam apenas os dados estritamente necessários, que são adequadas e proporcionais em relação à sua finalidade.

Tais limitações, junto com o fato de a lei assumir como regra a eliminação dos dados uma vez encerrado seu tratamento e de considerar o risco presente no tratamento de dados, indicam que a LGPD busca minimizar as hipóteses de tratamento àquelas que são úteis e necessárias, garantindo que mesmo estas sejam passíveis de restrição caso representem risco aos direitos e liberdades do titular. Trata-se, assim, de uma regulação que tem entre seus fundamentos principais a diminuição do risco, intrínseco ao tratamento de dados para o titular.

A lei prevê ainda especificações quanto à responsabilidade de determinados agentes. No caso do operador, só haverá responsabilização por atos que sejam contrários à lei ou às instruções fornecidas pelo controlador; neste último cenário, aplica-se o regime de responsabilidade solidária entre controlador e operador. Nas demais hipóteses, a responsabilidade cabe ao controlador.

Já no que diz respeito à responsabilidade administrativa, a LGPD estabelece uma série de sanções que, em caso de violação à lei, devem ser aplicadas pela autoridade nacional de proteção de dados. Tais sanções variam de uma advertência ou multa no valor de até 2% do faturamento da empresa no Brasil à proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados. Como parâmetro para o estabelecimento das sanções, a lei determina que seja considerada a adoção demonstrada de mecanismos e procedimentos internos voltados ao tratamento seguro e adequado de dados; de políticas de boas práticas e de governança; e de medidas corretivas.

Ao aplicar as sanções administrativas da LGPD, a autoridade deve levar em conta os critérios legais que informam se determinado tratamento de dados é irregular. Este é o caso quando o tratamento deixa de observar a legislação ou não fornece a segurança que o titular espera dele, consideradas as circunstâncias relevantes: o modo como o tratamento é realizado; o resultado e riscos esperados; as técnicas de tratamento de dados à disposição, entre outros.

Dessa forma, o terceiro nível do modelo de proteção de dados dialoga diretamente com os dois primeiros: em caso de descumprimento das condições de legitimidade de tratamento ou dos procedimentos para a proteção dos dados pessoais, os agentes de tratamento ficam sujeitos às sanções administrativas e ao pagamento de indenização ao titular. O objetivo dessa etapa é conferir efetividade

(...) em caso de descumprimento das condições de legitimidade de tratamento ou dos procedimentos para a proteção dos dados pessoais, os agentes de tratamento ficam sujeitos às sanções administrativas e ao pagamento de indenização ao titular.

Se, por um lado, o regime legal de proteção de dados é essencial para assegurar a autodeterminação do cidadão em relação ao fluxo de seus dados e para garantir a segurança jurídica de empresas e entidades que tratam dados pessoais, por outro lado, nem sempre ele será suficiente para impedir as violações cometidas pelo próprio legislador.

às normas previstas na LGPD, seja por meio da reparação de eventuais danos morais e materiais causados pelo descumprimento da lei, seja por meio da aplicação de sanções administrativas que buscam inibir o comportamento vedado pela legislação.

Próximos passos: tutela constitucional e fortalecimento institucional

A Lei Geral de Proteção de Dados Pessoais constituiu um grande avanço rumo à construção de um sistema de proteção de dados pessoais no Brasil, passo fundamental para o fortalecimento da confiança do cidadão nos serviços presentes na sociedade da informação e para o incentivo à inovação constante desses serviços. Contudo, é igualmente primordial a consolidação da tutela constitucional dos dados pessoais no ordenamento brasileiro.

Se, por um lado, o regime legal de proteção de dados é essencial para assegurar a autodeterminação do cidadão em relação ao fluxo de seus dados e para garantir a segurança jurídica de empresas e entidades que tratam dados pessoais, por outro lado, nem sempre ele será suficiente para impedir as violações cometidas pelo próprio legislador. A LGPD não está apta a proteger o cidadão de outras leis que venham a ser aprovadas pelo Poder Legislativo e que violem a sua privacidade, ao permitir, por exemplo, o processamento de dados abusivos, legitimar práticas de vigilância ou produzir discriminação por meio do processamento de dados. Basta pensar, por exemplo, em uma lei que autorize a utilização de dados raciais como *input* de um algoritmo criado para a identificação de devedores da Fazenda ou, ainda, uma lei que legitime a vigilância irrestrita da população pelo governo sem qualquer justificativa. Nessas situações, a mera existência de uma Lei Geral de Proteção de Dados Pessoais e de uma autoridade nacional não seria suficiente para resguardar os direitos dos cidadãos.

Nesse contexto, a Constituição brasileira apresenta dois importantes mecanismos de tutela da personalidade contra o tratamento indevido de dados: o direito material à proteção de dados pessoais e a garantia instrumental para a proteção desse direito, vinculada à ação do *habeas data*. A partir dessas experiências e da vivência institucional relacionada à proteção de dados no Brasil, hoje é possível reconhecer um direito fundamental à proteção de dados pessoais – a chamada autodeterminação informativa – como uma dimensão material do *habeas data* amparada na inviolabilidade da intimidade, da vida privada e da dignidade humana, nos termos da Constituição.

Para além da consolidação de uma tutela constitucional de proteção de dados, a efetiva implementação da Lei Geral de Proteção de Dados Pessoais dependerá da constituição de uma autoridade de proteção de dados pessoais que encontre apoio em um tripé consistente em poder sancionatório, *expertise* e independência. Sem a construção dessa arquitetura regulatória, não será possível alcançar o seu principal objetivo, que é o de consolidar a confiança da sociedade na infraestrutura de informação e comunicação, garantindo direitos, ampliando a inovação e propiciando mais competitividade entre os serviços que utilizam dados pessoais de forma legítima e transparente.

Nas últimas décadas, ficou claro que a existência de órgãos administrativos de proteção de dados pessoais é essencial para a implementação da legislação e da cultura da privacidade no Brasil. Nas palavras de Bennett e Raab (2006): "A existência de autoridades supervisoras robustas tem sido considerada como

condição *sine qua non* para a adequada proteção à privacidade, pois as leis não são autoimplementáveis e a cultura da privacidade não pode se estabelecer sem uma autoridade que a patrocine".

REFERÊNCIAS

Bennett, C. & Raab, C. (2006). *The Governance of Privacy*: Policy Instruments in Global Perspective. Cambridge: MIT.

Bennett, C. & Raab, C. (2018). *Revisiting 'The Governance of Privacy'*: Contemporary Policy Instruments in Global Perspective. Recuperado: 16 de maio de 2019, de ssrn.com/abstract=2972086.

Bioni, B. R. (2014). A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. *Direitos e novas tecnologias*: XXIII Encontro Nacional do Conpedi, v. 1, pp. 59-82.

Hartmann, M. & Wimmer, J. (2011). Einleitung. In Hartmann, M. & Wimmer, J. (Eds.), *Digitale Medientechnologien*: Vergangenheit – Gegenwart – Zukunft (pp. 21). Wiesbaden: VS.

Manifesto pela aprovação da Lei de Proteção de Dados Pessoais. (2018). São Paulo. Recuperado de brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais.

Mattern, F. (2008). Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In Roßnagel, A. et al. *Digitale Visionen*: Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlim: Springer.

Mendes, L. S. (2014). *Privacidade, proteção de dados pessoais e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva.

Mendes, L. S. & Doneda, D. (2016). Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, v. 9.

Entrevista I

P.S._ Na sua visão, quais são os principais atores e as dinâmicas que compõem o ecossistema de governança e regulação dos dados pessoais?

B.B._ Por um lado, há o titular, o próprio cidadão detentor daquela informação a ele vinculada, a ele correspondente – por isso, dados pessoais. Por outro lado, há os agentes de tratamento desses dados, que são as organizações que coletam e manejam as informações, como os setores privado e público. Existe uma subdivisão dentro desses agentes: o controlador, isto é, quem determina como os dados serão tratados. Em alguns cenários, ele terceiriza parte do tratamento dos dados. Nesses casos, entra em cena a figura do operador, cujo exemplo mais conhecido são as empresas contratadas para fazer o serviço de armazenamento dos dados, como as de computação em nuvem (*cloud computing*). Ainda para compor essa constelação de atores há os próprios órgãos reguladores. Nesse quesito, uma peça central da nova Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira é a criação de uma autoridade nacional de proteção de dados pessoais. O novo órgão terá como missão lidar com essa pauta e irá se juntar a outras agências reguladoras que têm essa responsabilidade dentro de seus respectivos setores, como a Secretaria Nacional do Consumidor. Um dos grandes desafios é promover a sinergia entre esses órgãos reguladores e, nesse sentido, o papel da futura autoridade nacional na coordenação da aplicação e fiscalização da LGPD com os demais atores será essencial. Por último, podemos citar as entidades de defesa de direitos difusos e coletivos. Em geral, o cidadão não tem no plano individual uma capacidade tão eficiente

Bruno Bioni
Consultor independente em privacidade e proteção de dados pessoais. Fundador do Data Privacy Brasil.

O Brasil já possui leis setoriais de proteção de dados pessoais, como no Código de Defesa do Consumidor, no Marco Civil da Internet, na Lei do Cadastro Positivo e na Lei de Acesso à Informação. Com a criação de uma lei geral, teremos um ordenamento jurídico regulatório mais completo, portanto, uma legislação de proteção de dados pessoais.

para a proteção de seus próprios direitos. Por isso, surgem organizações não governamentais que fazem a defesa de direitos em nome de grupos, além de outros órgãos, como a Defensoria Pública, o Ministério Público e os Procons. No cenário futuro, a tendência é que essas entidades lidem cada vez mais com uma agenda de proteção de dados pessoais.

P.S._ Na sua opinião, quais são os principais pontos da nova LGPD?

B.B._ O Brasil já possui leis setoriais de proteção de dados pessoais, como no Código de Defesa do Consumidor, no Marco Civil da Internet, na Lei do Cadastro Positivo e na Lei de Acesso à Informação. Com a criação de uma lei geral, teremos um ordenamento jurídico regulatório mais completo, portanto, uma legislação de proteção de dados pessoais. Por si só, a LGPD é importante porque, diferentemente dessas outras leis, ela é vocacionada para lidar somente com a proteção de dados pessoais. Assim, a LGPD elenca dez princípios que devem orientar qualquer tipo de tratamento de dados pessoais. Caso não haja o cumprimento de todos os dez princípios, o tratamento de dados pessoais será considerado ilegal.

Há agora um rol mais amplo de bases legais para o tratamento da proteção de dados pessoais, que são as autorizações e as hipóteses previstas pela LGPD que legitimam o tratamento dos dados. Essa lei é importante porque vai muito além do consentimento, a única base legal nas leis setoriais brasileiras. Com a LGPD, são adicionadas outras nove bases legais.

Um destaque é o legítimo interesse, passível de ser tomado como base por organizações em situações em que não seria possível obter consentimento, seja porque não há ponto de contato com o titular do dado, seja porque não seria recomendável buscar tal autorização. Isso poderia ocorrer, por exemplo, em atividades para a prevenção de fraude bancária. Está dentro do legítimo interesse de um banco evitar fraudes; ao mesmo tempo, como titular correntista do banco, é de meu benefício e está sob minha legítima expectativa que a instituição financeira trate meus dados pessoais sem o meu consentimento para gerar um perfil comportamental que sirva de critério para identificar operações financeiras possivelmente fraudulentas e, com isso, criar um sistema que previna fraudes. Esse é um típico caso de aplicação do legítimo interesse no qual há mais flexibilidade para autorizar o tratamento de dados pessoais.

Vale salientar ainda a aproximação da lei com ferramentas importantes de *compliance*, promovendo a existência de uma documentação por meio da qual organizações dos setores público e privado demonstram a sua conformidade com a LGPD. Hoje em dia, a principal ferramenta é o relatório de impacto da produção de dados pessoais, que indica o fluxo de dados tratados pela organização e aponta as respectivas bases legais, assim como as ações tomadas para atender à lei. É importante olhar para essa ferramenta de *compliance* como um documento por meio do qual as organizações

prestam contas sobre a sua conformidade com a lei, o que dialoga com um dos dez princípios da LGPD. Não adianta a organização dizer que faz um uso responsável dos dados pessoais; é preciso que ela documente esse processo de modo que, no futuro, possa demonstrar seu estado de conformidade com a LGPD.

P.S._ Qual é o impacto da General Data Protection Regulation (GDPR)[6] na América Latina?

B.B._ De maneira geral – e isso não é privilégio da GDPR –, ela tem aplicação extraterritorial, ou seja, a lei segue o dado, independentemente de onde esteja situado quem trata aquele dado. Para uma organização na América Latina que queira acessar o mercado europeu por meio da venda de produtos ou serviços, caso isso envolva tratamento de dados pessoais, a GDPR se aplica. Isso impacta a América Latina e o próprio cenário brasileiro de forma significativa, pois muitas das organizações locais têm, em menor ou maior medida, interface com o mercado da União Europeia.
Outro impacto diz respeito ao livre fluxo informacional, que está ligado a de que maneira os países trocam dados pessoais. Isso serve para os dois lados, ou seja, como as empresas brasileiras conseguem trazer dados coletados de pessoas situadas na União Europeia e como as empresas europeias conseguem transferir dados coletados de pessoas no Brasil. Por isso denominou-se de movimento bilateral. Na maioria das leis de proteção de dados pessoais – incluindo a GDPR e a LGPD –, há o livre fluxo informacional quando um país reconhece que o outro possui um nível adequado de proteção de dados pessoais. No futuro, algo que será tema de grande discussão no Brasil é a convergência entre a regulamentação brasileira e a europeia para que haja essa troca livre de dados. É por esse motivo que as leis de proteção de dados pessoais têm relação direta com a agenda de comércio exterior: em um cenário em que uma série de produtos e serviços depende do tratamento de dados pessoais e de sua transferência para viabilizar operações em um sentido global, essas leis têm um impacto importante.

P.S._ Na sua opinião, as legislações nacionais são suficientes para garantir o respeito à privacidade e a proteção dos dados pessoais? Existem outros mecanismos necessários?

B.B._ O código da lei, por si só, não é garantia de que aquilo que está previsto terá aderência na realidade. Na perspectiva de se pensar uma caixa de ferramentas para modular comportamentos na sociedade, o direito e

Não adianta a organização dizer que faz um uso responsável dos dados pessoais; é preciso que ela documente esse processo de modo que, no futuro, possa demonstrar seu estado de conformidade com a LGPD.

[6] General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados) é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais aplicável a todos os indivíduos na União Europeia (UE) e no Espaço Econômico Europeu (EEE). Regulamenta também a exportação de dados pessoais para fora da UE e EEE.

(...) a lei é apenas uma das ferramentas e, sozinha, não é suficiente para garantir o respeito à privacidade e a proteção dos dados pessoais. É preciso que ela seja articulada ao interesse econômico – o mercado –, ao aspecto cultural – as normas sociais – e à tecnologia. Aí, sim, será possível falar de uma proteção eficiente de dados pessoais.

as leis são apenas uma delas. Há outras ferramentas possíveis, como o próprio mercado, uma vez que ele pauta uma série de comportamentos sociais. Nesse sentido, uma grande mudança é as organizações enxergarem na privacidade e na proteção de dados pessoais uma vantagem competitiva, uma questão reputacional. Quando passa a existir um grupo de organizações que vocaliza como diferencial a proteção efetiva das informações de seus consumidores, o mercado emerge como um instrumento de modulação dos comportamentos.

Outra ferramenta são as próprias normas sociais, ou seja, como a sociedade constrange determinados comportamentos por si mesma, independentemente do Legislativo e do mercado. Isso está ligado a um aspecto cultural: nos países ou ambientes em que há uma cultura de proteção de dados pessoais, a própria sociedade exige do setor público – enquanto regulador ou grande interessado em tratar os dados – e do setor privado boas práticas para a proteção dos dados.

Por último, há a tecnologia, ou seja, como ela pode reforçar ou neutralizar a nossa capacidade de controlar as informações que nos dizem respeito. Um exemplo clássico é a criptografia, que reforçou o controle sobre nossos dados, sobretudo ao manter sigilo sobre o conteúdo das comunicações entre remetente e destinatário, onde se encontra uma série de dados pessoais. Existem também tecnologias que vão no sentido contrário, como as de reconhecimento facial, que permitem não só identificar uma determinada pessoa no meio de uma multidão, mas também reconhecer emoções e aspectos comportamentais por meio das expressões faciais. Portanto, a lei é apenas uma das ferramentas e, sozinha, não é suficiente para garantir o respeito à privacidade e a proteção dos dados pessoais. É preciso que ela seja articulada ao interesse econômico – o mercado –, ao aspecto cultural – as normas sociais – e à tecnologia. Aí, sim, será possível falar de uma proteção eficiente de dados pessoais.

P.S._ Muito se discute sobre o uso de dados pessoais por grandes empresas como Facebook e Google. De maneira geral, como o setor privado coleta e utiliza nossos dados?

B.B._ Uma primeira colocação é que a LGPD e, de modo geral, as regras de proteção de dados pessoais vão muito além do ecossistema da Internet, principalmente quando consideramos as organizações cujos modelos de negócios são baseados no uso de dados pessoais para o direcionamento de publicidade, conteúdo, entre outros. Setores tradicionais da economia, como a indústria automobilística, o setor de saúde e o de energia elétrica, têm cada vez mais apostado no uso dos dados de sua audiência,

consumidores e público-alvo para otimizar a prestação de serviços e fazer uma modelagem mais precisa dos produtos antes de seu lançamento no mercado. Então, em termos gerais, podemos dizer que boa parte do setor privado coleta e utiliza nossos dados pessoais para gerar competitividade e mais eficiência em suas atividades econômicas.

Algo que aparenta ser uma tendência é o entendimento pelo próprio setor privado da proteção de dados pessoais como valor, sobretudo, de ordem reputacional. Uma das questões que a LGPD traz é o direito de portabilidade, que permite ao titular migrar junto com seus dados para um serviço concorrente. Dentro dessa possibilidade, começamos a olhar para um cenário em que a proteção de dados pessoais aparece como um diferencial competitivo, o que é uma grande janela de oportunidade para o setor privado reconhecer o valor dessa mensagem de proteção e uso responsável dos dados enquanto uma estratégia de negócios.

P.S._ E o que acontece no âmbito dos provedores de serviço de Internet?

B.B._ A maioria dos modelos de negócios que existem hoje na Internet se baseia na publicidade comportamental. O consumidor ou usuário do serviço não paga por ele em dinheiro, mas faz uma "troca" de seus dados para que esse modelo de negócios seja monetizado pela entrada de publicidade comportamental em uma rede social ou um mecanismo de busca, por exemplo. Esse é um ecossistema bastante impactado por qualquer lei de proteção de dados pessoais. No Brasil não será diferente. Daqui para frente, precisamos observar o comportamento desses atores. Nesse cenário, tal como aconteceu na União Europeia, temos o papel das associações de classe em convocar todos esses atores a pensar boas práticas para que a própria reputação do setor seja responsiva às normas de proteção de dados pessoais. Isso significa, por exemplo, pensar como as tecnologias podem gerar padrões interoperáveis nessa multidão de atores para que, uma vez assinalada a opção do que você quer que seja ou não feito com seus dados, essa decisão seja alcançável e gere uma trilha auditável ao longo de todo o ecossistema de mídia *on-line*. O grande dilema, especificamente no âmbito da Internet, é que quando você utiliza essas plataformas, diversos atores estão acompanhando, monitorando e colecionando uma série de informações sobre seus hábitos para formar um perfil comportamental bastante preciso sobre você. Não é por acaso que uma determinada publicidade passa a te acompanhar em vários ambientes que você frequenta na Internet. Dessa forma, a questão que se coloca é conseguir desenvolver tecnologias capazes de escalar a capacidade do titular de ter mais controle e visão da maneira como seus dados são trafegados nesses ambientes, como isso se volta para eles, seja enquanto direcionamento de conteúdo ou de publicidade.

O consumidor ou usuário do serviço não paga por ele em dinheiro, mas faz uma "troca" de seus dados para que esse modelo de negócios seja monetizado pela entrada de publicidade comportamental em uma rede social ou um mecanismo de busca, por exemplo.

Entrevista II

Joana Varon
Diretora Executiva da Coding Rights.

P.S._ Qual é a importância da proteção de dados pessoais? Por que pode ser problemático que um terceiro tenha o histórico de minhas compras, informações médicas, orientação sexual ou religião?

J.V._ Proteção de dados significa poder escolher quem tem acesso às nossas informações e em quais circunstâncias, ou seja, decidir o que compartilhar e saber como os dados são utilizados por empresas, governo e outras organizações. Esse controle é importante para garantir direitos, não apenas à privacidade, mas também à liberdade de expressão, ao desenvolvimento da nossa personalidade, até mesmo à igualdade e contra a discriminação. Isso porque, à medida que gradualmente se usa dados pessoais para alimentar processos de tomada de decisão, seja de maneira automática (por meio de algoritmos) ou manual, tornam-se mais importantes a transparência e o controle de nossos dados para saber se estamos sendo discriminados em razão das práticas de perfilamento (*profiling*) feitas com base nas informações que estão disponíveis sobre nós.
Por exemplo, ao fornecer o número do CPF para obter descontos nas farmácias, a lista de medicamentos associada a esse dado pode conter informações delicadas sobre nossa saúde. É possível que essas informações sejam utilizadas de maneira discriminatória por seguradoras de saúde, alterando o valor da franquia de acordo com o perfil. Da mesma forma, nosso histórico de compras *on-line* diz bastante sobre poder aquisitivo e preferências pessoais. Por meio dessas informações, é possível embasar o direcionamento de propagandas compatíveis com o nosso gosto, tentando-nos a comprar algo que não precisamos, bem como cobrar preços mais altos ou limitar o acesso ao crédito para determinados perfis. Dados sobre orientação sexual, em uma sociedade que ainda vive preconceitos contra a diversidade, também podem servir a práticas de segregação, restringindo, por exemplo, as oportunidades de trabalho. No projeto chupadados.com, trazemos histórias sobre usos cotidianos dos nossos dados pessoais e algumas implicações disso em nossas vidas.

P.S._ O que implica "aceitar os termos de uso" de um aplicativo ou um site? Ao fazê-lo, estamos consentindo com o quê? Quais são os direitos do usuário?

J.V._ Cada termo de uso ou política de privacidade tem implicações distintas. Um aplicativo pode ser mais ou menos cuidadoso com o manejo dos dados e, portanto, com a privacidade e a segurança. O problema é que na maioria das vezes apenas clicamos no botão de "Aceito" sem lê-los, até porque eles não foram feitos de maneira a facilitar a leitura. Acabamos consentindo com algo que sequer sabemos o que é. Se o responsável pelo desenvolvimento do aplicativo não tiver qualquer preocupação com nossa privacidade ou se o uso dos dados for parte de seu modelo de negócios, é muito provável que os dados sejam compartilhados com terceiros ou utilizados para práticas de perfilamento.

P.S._ Como nossos dados pessoais podem ser usados para "alimentar" os algoritmos? Quais são as implicações disso?

J.V._ Os algoritmos têm sido utilizados cada vez mais no nosso cotidiano, em inúmeros momentos em que transferimos para o computador os processos de tomada de decisão. Eles decidem o que mostrar quando fazemos uma busca no Google ou se a próxima postagem que visualizaremos na *timeline* será uma propaganda de passagem aérea ou de roupa de bebê. Eles apontam se o seu dedo é realmente seu no reconhecimento biométrico do banco ou, em alguns testes polêmicos de reconhecimento facial realizados durante as festas de carnaval deste ano, se uma pessoa que passa diante de uma câmera é alguém que integra a base de dados da polícia. Em breve, eles vão nos substituir na direção de veículos.
Algoritmos nada mais são do que uma sequência de passos programados para realizar uma tarefa. Os exemplos acima ilustram algoritmos que otimizam análises de dados para uma tomada de decisão. O problema é que nem sempre a decisão é ótima. Dependendo de como os algoritmos são programados, as bases de dados organizadas e os passos do processo valorados, o resultado pode reforçar assimetrias, preconceitos e desigualdades. O livro *Algorithms of Oppression*, de Safiya Umoja Noble, demonstra como mecanismos de busca reforçam práticas racistas e machistas, sugerindo termos pejorativos como complementação automática da busca digitada. O mesmo acontece com tecnologias de reconhecimento facial, que tendem a apontar falsos positivos para rostos de mulheres, principalmente negras[7]. Isso ocorre porque quem desenha esses algoritmos replica as estruturas de poder predominantes na sociedade.

P.S._ O que podemos fazer para usar redes sociais, aplicativos, plataformas de serviços e, ao mesmo tempo, proteger nossos dados pessoais?

J.V._ O primeiro passo é tomar consciência de que essas tecnologias funcionam por meio do processamento dos nossos dados, muitas vezes lucrando com eles. Podemos optar por aplicativos e serviços que, entre outros aspectos, têm a privacidade e a segurança como valores do produto oferecido; que garantem proteções como o uso de criptografia; que promovem a minimização das informações coletadas e armazenadas ao longo do tempo; que não compartilham dados com terceiros, a não ser por requisições legais; que têm código aberto; e que não exigem autenticações com o nome verdadeiro ou outra forma de identificação.
No caso de redes sociais e outros serviços que não são pautados por essas preocupações, mas que, ainda assim, precisamos usar, é aconselhável fazer uma gestão de identidade, ou seja, avaliar que tipo de dados pessoais desejamos associar a cada uma de nossas personas. Também é indicado checar as configurações de privacidade e ajustá-las para minimizar a coleta

Dependendo de como os algoritmos são programados, as bases de dados organizadas e os passos do processo valorados, o resultado pode reforçar assimetrias, preconceitos e desigualdades.

[7] Em uma audiência pública na Câmara dos Deputados em 03 de abril deste ano, foram elencados estudos críticos sobre o uso dessas tecnologias para a segurança pública. Para saber mais, acesse medium.com/codingrights/bem-na-sua-cara-a-ilus%C3%A3o-do-reconhecimento-facial-para-seguran%C3%A7a-p%C3%Bablica-47c708b34820

Quando um produto considera *Privacy by Default*, ele é lançado com as configurações de privacidade mais protetivas por padrão, ou seja, você tem de optar se deseja guardar ou compartilhar seus dados; é o contrário da lógica vigente.

e o armazenamento de dados. Ao mesmo tempo, recomenda-se cada vez mais garantir formas autônomas de gestão dos dados pessoais – por exemplo, ter o próprio conteúdo em outros locais que não apenas as redes sociais.

P.S._ O que significam os conceitos de "Privacy by Design" e "Privacy by Default"? Como os desenvolvedores podem adotar esses princípios para desenvolver aplicações que protejam a privacidade do usuário?

J.V._ Hoje, pelo fato de a lógica dominante no desenvolvimento de muitas tecnologias, principalmente (mas não só) para a Web, ser a lógica do capitalismo de dados, a maioria dos produtos e serviços tem como padrão configurações que permitem a coleta massiva de dados e seu armazenamento. Quando um produto considera *Privacy by Default*, ele é lançado com as configurações de privacidade mais protetivas por padrão, ou seja, você tem de optar se deseja guardar ou compartilhar seus dados; é o contrário da lógica vigente. Já *Privacy by Design* é um conceito ainda mais amplo, que significa que os produtos ou serviços levaram em conta a preocupação com a privacidade desde o início de seu desenvolvimento. É o caso de serviços desenvolvidos por coletivos e grupos que seguem o que antes se chamava de lógica *cypherpunk*, valorizando a criptografia forte e a proteção da privacidade. Por exemplo, o Signal, aplicativo de mensagens que serve de alternativa a produtos altamente invasivos como o WhatsApp, ou o Tor, navegador que preza pelo anonimato do usuário.

P.S._Quais técnicas são recomendadas para manter os dados pessoais protegidos?

J.V._ Não há uma receita única – depende de quem somos, o que, quando, onde e para quem comunicamos. Temos diferentes medidas para proteger tanto nossas comunicações como nossos dados pessoais. Em geral, as técnicas são associadas a práticas que dizem respeito à proteção dos dados (por exemplo, o uso de criptografia), à minimização da quantidade de dados coletados ou armazenados e à gestão de identidade (ou seja, o ato de separar nossas diferentes personas entre diversas identidades *on-line*).
Por outro lado, existem situações em que não temos escolha, pois nossos dados são requeridos, por exemplo, para acessar serviços públicos. Em todos os casos que dizem respeito à gestão dos nossos dados, podemos usar ferramentas de transparência para saber o que é feito com as informações, como o *habeas data*, e eventualmente requerer correções ou mesmo compensações pelo uso indevido. Nesse sentido, é fundamental que a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira entre em vigor também com a previsão de uma autoridade de proteção de dados, que sirva como fiscalizadora de práticas tanto do setor público como do setor privado.

Relatório de Domínios

A dinâmica dos registros de domínios no Brasil e no mundo

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) monitora mensalmente o número de nomes de domínios registrados entre os 16 maiores domínios de topo de código de país (do inglês, *country code* Top-Level Domain – ccTLD) no mundo. Somados, eles ultrapassam 101,3 milhões de registros[8]. Em maio de 2019, os domínios registrados sob .tk (Tokelau) chegaram a 23,7 milhões. Em seguida, aparecem Alemanha (.de), China (.cn) e Reino Unido (.uk), com, respectivamente, 16,2 milhões, 11,7 milhões e 9,7 milhões de registros. O Brasil teve 4 milhões de registros sob .br, ocupando a sétima posição. Na 16ª posição, com 1,9 milhão de registros, está a Espanha (.es), como observado na Tabela 1.

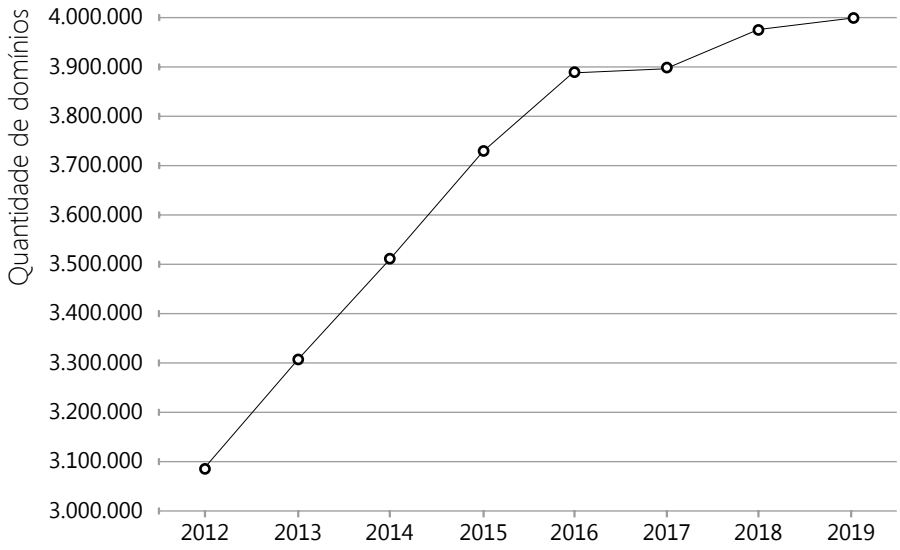
TABELA 1 – REGISTRO DE NOMES DE DOMÍNIOS NO MUNDO – MAIO/2019

Posição	ccTLD	Domínios	Ref.	Fonte
1	Tokelau (.tk)	23.704.267	Mai/19	research.domaintools.com/statistics/tld-counts
2	Alemanha (.de)	16.224.416	Mai/19	www.denic.de
3	China (.cn)	11.719.947	Mai/19	research.domaintools.com/statistics/tld-counts
4	Reino Unido (.uk)	9.778.572	Mai/19	www.nominet.uk/uk-register-statistics-2018
5	Países Baixos (.nl)	5.852.144	Mai/19	www.sidn.nl
6	Rússia (.ru)	5.014.569	Mai/19	www.cctld.ru
7	**Brasil (.br)**	**4.040.132**	**Mai/19**	**registro.br/estatisticas.html**
8	União Europeia (.eu)	3.582.957	Mai/19	research.domaintools.com/statistics/tld-counts
9	França (.fr)	3.377.847	Mai/19	www.afnic.fr/en/resources/statistics/detailed-data-on-domain-names
10	Itália (.it)	3.197.556	Mai/19	www.nic.it
11	Austrália (.au)	3.187.548	Mai/19	www.auda.org.au
12	Canadá (.ca)	2.831.137	Mai/19	www.cira.ca
13	Polônia (.pl)	2.616.373	Mai/19	www.dns.pl/english/zonestats.html
14	Suíça (.ch)	2.215.837	Abr/19	www.nic.ch/reg/cm/wcm-page/statistics/index.html?lid=em*
15	Estados Unidos (.us)	2.054.778	Mai/19	research.domaintools.com/statistics/tld-counts
16	Espanha (.es)	1.926.092	Mai/19	www.dominios.es

[8] É importante destacar que há variação entre o período de referência dos ccTLDs, embora seja sempre o mais atualizado para cada país.

O Gráfico 1 apresenta o desempenho do .br desde o ano de 2012.

Gráfico 1 – TOTAL DE REGISTROS DE DOMÍNIOS AO ANO DO .BR – 2012 a 2019*



**Dado referente ao mês de maio de 2019.*
Fonte: Registro.br

Em maio de 2019, os cinco principais domínios genéricos (do inglês, *generic Top-Level Domain* – gTLD) totalizaram mais de 172 milhões de registros. Com 141,6 milhões de registros, destaca-se o .com, conforme apontado na Tabela 2.

Tabela 2 - PRINCIPAIS GTLDS - MAIO/2019

Posição	gTLD	Domínios	Fonte	Ref.
1	.com	141.602.087	research.domaintools.com/statistics/tld-counts	mai/19
2	.net	13.561.131	research.domaintools.com/statistics/tld-counts	mai/19
3	.org	10.199.035	research.domaintools.com/statistics/tld-counts	mai/19
4	.info	4.740.206	research.domaintools.com/statistics/tld-counts	mai/19
5	.biz	2.033.621	research.domaintools.com/statistics/tld-counts	mai/19

Fonte: DomainTools.com. Recuperado de: research.domaintools.com/statistics/tld-counts

O QUE VOCÊ SABE SOBRE METADADOS?

EM UMA CARTA

As informações no envelope são os metadados. O que vai dentro dele é o conteúdo.

EM UM TELEFONEMA

A hora da chamada, sua duração, a geolocalização dos dispositivos e o número dos participantes são alguns dos metadados. O conteúdo é o que é conversado.

AO VISITAR UM *SITE*

Os metadados são seu endereço de IP, a hora de acesso ao *site*, a duração da visita, as características do equipamento e a partir de onde você está se conectando. O conteúdo é o que aparece na tela.

Quando são acumulados muitos metadados de uma pessoa, seus padrões de comportamento começam a aparecer: é possível saber onde ela mora, com quem se encontra, quais são seus interesses e opiniões, sem existir a necessidade de acessar o conteúdo de suas comunicações.

Fonte: Adaptado de Viera, C. (2017). Recuperado de www.derechosdigitales.org/tipo_publicacion/infografias

QUAIS INFORMAÇÕES OS METADADOS ENTREGAM SOBRE VOCÊ?

Os metadados são um conjunto de informações que descrevem um conteúdo.

Fonte: Adaptado de Figueroa, C. e Garay, V. (2015). Recuperado de www.derechosdigitales.org/publicaciones/que-informacion-entregan-los-metadatos-sobre-ti

/Créditos

REDAÇÃO
ARTIGO PRINCIPAL
Laura Mendes
(UnB/IDP)

RELATÓRIO DE DOMÍNIOS
José Márcio Martins Júnior
(Cetic.br)

COORDENAÇÃO EDITORIAL
Alexandre Barbosa
(Cetic.br)
Tatiana Jereissati
(Cetic.br)
Stefania L. Cantoni
(Cetic.br)

AGRADECIMENTOS
Laura Mendes
(UnB/IDP)

Bruno Bioni
(Data Privacy Brasil)

Joana Varon
(Coding Rights)

REVISÃO EM PORTUGUÊS
Mariana Tavares

PROJETO GRÁFICO E DIAGRAMAÇÃO
Comunicação NIC.br

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

cetic.br
Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação sob os auspícios da UNESCO

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

POR UMA INTERNET CADA VEZ MELHOR NO BRASIL

CGI.BR, MODELO DE GOVERNANÇA MULTISSETORIAL

www.cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK