FGV DIREITO SP

GRUPO DE ENSINO E PESQUISA EM INOVAÇÃO

Coordenação do GEPI:

Professora Mônica Steffen Guise Rosina
Professor Alexandre Pacheco da Silva

Equipe de Pesquisa:

Rodrigo Moura Karolczak
Carlos Augusto Liguori Filho
Luiz Fernando Prado
Carla Segala
Plínio Kentaro de Britto Costa Higasi

Objeto:

Contribuição do Grupo à minuta de Decreto que regulamenta a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet)

Sumário:

1. Apresentação do GEPI

O Grupo de Ensino e Pesquisa em Inovação (GEPI) foi criado em 2011 na Escola de Direito de São Paulo da Fundação Getulio Vargas (FGV Direito SP) pela Professora Mônica Steffen Guise Rosina com o objetivo geral de aprofundar os debates sobre como novas tecnologias podem transformar o arcabouço jurídico-institucional do Brasil.

Desde o início de suas atividades, o GEPI voltou grande parte de seus esforços de pesquisa à regulação da Internet no Brasil, identificando no debate um ambiente profícuo para reflexões sobre modelos normativos adequados ao enfrentamento dos desafios tecnológicos no país.

Nos últimos cinco anos, o GEPI buscou expandir suas linhas de pesquisa e criar instâncias de debate sobre a relação entre Direito e Inovação Tecnológica dentro da FGV Direito SP. Foram criadas atividades de ensino no âmbito da graduação (Laboratório de Empresas Nascentes de Tecnologia – LENT), do programa de intercâmbio internacional (*Digital Democracy*), e do mestrado profissional (Direito e Novas Tecnologias). Além disso, o GEPI ampliou suas linhas de pesquisa, que em 2011 eram 2, passando para 6 em 2016. São elas:

(i) Democracia digital;
(ii) Discurso de ódio na Internet;
(iii) Flexibilização de direitos autorais;
(iv) Empreendedorismo e empresas nascentes de base tecnológica;
(v) Fashion law; e
(vi) Privacidade e proteção de dados pessoais.

No contexto de sua linha de pesquisa sobre privacidade e proteção de dados pessoais, o GEPI tem acompanhado os esforços realizados pelo Ministério da Justiça, com especial destaque para a Secretaria de Assuntos Legislativos e para a Secretaria Nacional do Consumidor, em criar um espaço de ampla participação e debate sobre qual modelo jurídico de proteção de dados pessoais a sociedade brasileira considera mais adequado para a Internet. No intuito de contribuir para esse debate, damos sequência à nossa participação por meio da avaliação da minuta do Decreto que regulamenta a Lei nº 12.965, de 23 de abril de 2014, proposta pela Presidência da República.

O GEPI acredita que pode melhor contribuir ao debate por meio de uma avaliação sobre aquilo que considera as principais fragilidades da minuta do Decreto, apontando para fatores que devem ser considerados e possíveis alternativas. Desde já deixamos claro que a minuta do Decreto guarda em si muitas virtudes ao apresentar um esforço de regulamentação do Marco Civil da Internet em três pontos extremamente importantes e sensíveis: neutralidade de rede, gestão de dados pessoais e segurança da informação.

A presente contribuição foi fruto do trabalho dos pesquisadores do GEPI que trabalham em regime de tempo integral na FGV Direito SP, bem das contribuições de especialistas em propriedade intelectual, hoje colaboradores externos do Grupo.

Quatro foram os eixos escolhidos para a contribuição do GEPI:

(i) Análise da estrutura da minuta do Decreto;
(ii) Problemas com a Terminologia utilizada;
(iii) Percepções conflitantes sobre tratamento e gestão de dados pessoais;
(iv) A importância do conceito de dado pessoal.

Para cada um dos eixos selecionados, a equipe do GEPI buscou embasamento teórico em artigos científicos, experiências internacionais de regulação da proteção de dados pessoais e modelos de gestão de dados pessoais. Todos os materiais utilizados estão referenciados e têm sua indicação completa ao final do documento.

Vale ressaltar que pelo fato de não dispormos de uma linha de pesquisa que se dedica ao estudo de neutralidade de rede não nos sentimos confortáveis em tecer comentários sobre o capítulo II da minuta de Decreto. Acreditamos que a minta receberá contribuições qualificadas de outras entidades de pesquisa e pesquisadores independentes que têm dedicado sua atenção ao tema de forma mais detalhada.

Por fim, este documento, mesmo oferecendo uma contribuição acadêmica para o debate público da minuta do Decreto, adotou uma estrutura menos formal e mais fluída de argumentação e exposição de dados empíricos capazes de qualificar o texto proposto. Por esta razão, a estrutura do texto e o estilo de apresentação de nossos argumentos distanciam-se da forma tradicional da escrita acadêmica.

O documento final é de total responsabilidade da equipe do GEPI e representa seu posicionamento neste debate.

2. Análise da estrutura da minuta do decreto

Em sentido amplo, desde a publicação da Lei n.º 12.965/2014 (Marco Civil da Internet - MCI) o GEPI nutriu expectativas quanto à sua regulamentação. No texto do diploma normativo há diversos temas que merecem um tratamento mais detalhado por parte do regulador, em especial no que tange à regulação da privacidade.

Todavia, o texto apresentado na minuta do Decreto que regulamentaria o Marco Civil da Internet surpreende, no mínimo, por dois problemas evidentes:

(i) o seu silêncio sobre temas aos quais o texto do Marco Civil expressamente menciona a necessidade de regulamentação; e

(ii) o caráter de novidade de algumas previsões no texto da minuta do Decreto, o que extrapolaria, em nossa visão, o escopo *regulamentador* do mesmo.

A presente seção dedicar-se-á a explorar os dois problemas apontados acima, reconhecendo o esforço que foi empregado pelos autores do texto em dar maior clareza ao texto do Marco Civil da Internet. Nesse sentido, nosso intuito com esta contribuição é auxiliar os responsáveis pela revisão do texto a aprimorá-lo, qualificando o debate que levará à regulamentação.

Na Lei n.º 12.965/2014 há pelo menos seis menções expressas à regulamentação: (i) parágrafo 1º do artigo 9º; (ii) parágrafo 4º do artigo 10; (iii) parágrafo 3º do artigo 11; (iv) parágrafo 4º do artigo 11; (v) *caput* do artigo 13; e (vi) *caput* do artigo 15. Nestes cinco dispositivos o uso das expressões "regulamento", "regulamentará" e "regulamentação" servem como guia ao agente infra-legal sob quais são os temas que demandam regulamentação.

Conforme mencionado na seção 1 desta contribuição, não iremos tratar dos dispositivos que cuidam da regulamentação das regras de neutralidade de rede presentes no Marco Civil da Internet. Por esta razão, limitamos nossa análise aos dispositivos legais relacionados à proteção de dados pessoais e a segurança da informação.

Dentre as demais menções expressas, nota-se que apenas o art. 10 e o parágrafo 3º do art. 11 do MCI foram regulamentados no texto do Decreto, mesmo que de forma incompleta em seu artigos 11, 13 e 14, deixando os demais dispositivos sem regulamentação. Trataremos dos problemas gerados pela regulamentação do art. 10 do MCI nas seções 4 e 5 desta contribuição. Nesta seção, trataremos dos dispositivos que foram relegados.

O primeiro exemplo da falta de regulamentação por parte do texto do Decreto encontra-se no parágrafo 4º[1] do art. 11 do MCI, que estabelece que o Decreto que regulamentará o MCI

[1] Conforme o texto do MCI "Art. 11 Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados

irá dispor sobre o procedimento para apuração de infrações relacionadas a operações de coleta, armazenamento, guarda e tratamento de registros e de dados pessoais.

Em nenhuma disposição do texto apresentado para consulta pública o Decreto descreve tais procedimentos de apuração de infrações. Em sua seção II (Padrões de Segurança e Sigilo dos Registros, Dados Pessoais e Comunicações Privadas), dedica-se a oferecer diretrizes para adoção e divulgação de padrões de segurança (art. 11), define dados pessoais e tratamento de dados pessoais (art. 12), trata da adoção de formatos mais acessíveis de dados (art. 13) e confere maior transparência na divulgação de informações de padrões de segurança da informação (art. 14).

Da mesma forma, **nota-se a ausência de definição das condições da guarda de registros de conexão** por parte de provedores de conexão prevista no *caput*[2] do art. 13 do MCI. Esperava-se que o Decreto enfrentasse quais seriam as características de um ambiente controlado e de segurança para a conservação destes registros. O disposto no art. 11 da minuta do Decreto posto em consulta pública não reflete o cuidado e a sofisticação dos debates nacionais e internacionais sobre segurança da informação.

Acrescente-se que a mesma crítica pode ser estendida à inexistência de regulamentação ao *caput* do art. 15 do MCI na minuta do Decreto, que reproduz a obrigação prevista no *caput* do art. 13 do MCI, só que agora para provedores de aplicação.

A opção de regulamentar no mesmo artigo (art. 11) quais devem ser os deveres de provedores de conexão e de aplicações de internet nos parece uma escolha equivocada, pois os serviços oferecidos por tais agentes são significativamente diferentes, conforme traduz o art. 5º do MCI, exigindo cuidados distintos para cada um deles. Da mesma forma, **não nos parece que os cuidados previstos nos incisos do art. 11 da minuta sejam diretrizes suficientemente precisas no âmbito da segurança da informação**.

Apenas a título de exemplo, a Cartilha de Segurança para a Internet[3], publicada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) em 2012, oferece um quadro muito mais sofisticado sobre segurança na internet do que a minuta, em especial por diferenciar tipos de risco na internet (golpes, ataques, códigos maliciosos e outras formas de coleta de dados, como cookies, códigos móveis, extensões, dentre outros).

Não há no texto proposto na minuta menção expressa de notificação de incidentes de segurança, hipóteses de abuso no uso de dados, bem como o texto não elucida o que são

---

pessoais e ao sigilo das comunicações privadas e dos registros. (...) §4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo."

[2] Nas palavras do MCI: "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento."

[3] Mesmo não sendo um documento técnico ou acadêmico, a cartilha produzida pelo CERT.Br traz conceitos, recomendações e exemplos ilustrativos sobre riscos relacionados à segurança da informação que podem auxiliar formuladores de políticas públicas que não detém o domínio da linguagem técnica da internet. Recomendamos a consulta ao documento, em especial na descrição que oferece sobre criptografia de dados e sobre as tecnologias de coleta e tratamento de dados, pois mesmo que não estejam na fronteira dos debates sobre proteção de dados, vale como guia para a reflexão sobre a regulação do tema. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Último acesso em 10.02.2016.

medidas de proteção equivalentes à criptografia de dados. Ferramentas *antimalware*, filtros *antispam*, cópias de segurança (*backups*) seriam tecnologias de proteção equivalentes? Pergunta que iremos explorar na seção 4 desta contribuição.

Além disso, há entidades internacionais de certificação de padrões de segurança que dispõe de diversos critérios para atestar a segurança na gestão de dados e informações em empresas e entidades da sociedade civil. O certificado ISO/IEC27001:2013 é um exemplo interessante, em particular porque oferece critérios de avaliação de risco na gestão de dados.

Nesse sentido, os incisos do art. 11 da minuta do Decreto **não são capazes de orientar os destinatários da norma**, empresas, entidades de pesquisa, sociedade civil, entre outros que realizam coleta e tratamento de dados, bem como **utiliza uma terminologia de difícil interpretação**, o que iremos explorar na seção 3 desta contribuição.

Recomendação 1: Acréscimo de um dispositivo específico com a descrição dos procedimentos para apuração de infrações relacionadas a coleta, armazenamento, guarda e tratamento de dados, conforme estabelecido no §4º do art. 11 do MCI.

Recomendação 2: Separação das diretrizes sobre padrões de segurança de dados a serem adotadas por provedores de conexão e provedores de aplicação de internet em artigos distintos, com a associação entre ferramenta de segurança recomendada com um risco a segurança específico.

Em relação ao segundo problema apontado nesta seção – o caráter de novidade de algumas previsões dispostas na minuta do Decreto – o texto suscitou diversas dúvidas, em especial sobre a função normativa de um Decreto que deve regulamentar o MCI. Por essa razão, recorremos a autores do direito administrativo para verificar se as inovações propostas no texto objeto de análise poderiam fazer parte de um Decreto.

Na definição clássica de Hely Lopes Meirelles[4], bem como na de Odete Medauar[5], Celso Antônio Bandeira de Melo[6] e Maria Sylvia Zanella de Pietro[7], Decreto é o ato administrativo ou a forma que se revestem os atos do Chefe do Poder Executivo em suas diferentes dimensões (Presidente da República, Governador e Prefeito), podendo conter, da mesma forma que a Lei, regras gerais dirigidas para pessoas ou grupo de pessoas determinadas. **Por definição, o Decreto nasce em situação inferior a Lei, não podendo contrariá-la**.

Segundo Maria Sylvia Zanella Di Pietro[8], o Decreto pode ser divido em duas categorias: (i) regulamentar, que busca a fiel execução do texto de uma Lei, conforme previsto no art. 84, inciso IV da Constituição Federal; e (ii) o autônomo, quando a matéria não exige sua

[4] MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. 41ª edição, atualizada até a Emenda Constitucional 84, de 2.12.2014. São Paulo Malheiros Editores, 2015, p. 198.
[5] MEDAUAR, Odete. Direito Administrativo Moderno. 18ª edição revista e atualizada. São Paulo: Revista dos Tribunais, 2014, p. 165.
[6] BANDEIRA DE MELLO, Celso Antônio. Curso de Direito Administrativo. 32ª edição revista e atualizada até a Emenda Constitutcional 84, de 2.12.2014. São Paulo: Malheiros Editores, 2015, p. 351.
[7] DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. Vigésima Sétima Edição. São Paulo: Atlas, 2013, p. 244.
[8] Idem, p. 245.

regulamentação por Lei e sua regulamentação não implique aumento nas despesas do Poder Público ou enseje a criação ou extinção de órgãos públicos.

Obviamente a minuta do Decreto colocado em consulta enquadra-se na categoria de diploma normativo regulamentar, tendo como característica ser ato normativo derivado, não podendo criar direito novo ou obrigações não previstas no texto de lei, e tendo como principal função o estabelecimento de normas que **viabilizem** a execução da Lei.

A este respeito, Celso Antônio Bandeira de Mello[9] chega a ser mais veemente ao afirmar que o princípio da legalidade impõe caráter de ato estritamente subordinado ao regulamento, **tornando-o integralmente dependente da Lei**. Na visão do administrativista, só a Lei é capaz de inovar, de criar deveres e obrigações na ordem jurídica nacional.

Para os fins da presente contribuição, não é nossa intenção explorar os pormenores do debate sobre a natureza jurídica de Decreto no ordenamento jurídico brasileiro. Contudo, acreditamos que retomar o conceito de Decreto pode nos ajudar a analisar duas inovações presentes na minuta que, em nossa visão, **extrapolam o poder normativo de um Decreto**, quais sejam: (i) o art. 9º da minuta, que versa sobre acesso e define dados cadastrais; e (ii) o art. 12, que conceitua dado pessoal e tratamento de dados.

O art. 9º da minuta encontra-se na Seção I – Da Requisição de dados cadastrais, definindo a obrigação de autoridades administrativas de indicar sua competência legal e sua motivação para pedidos de acesso a dados cadastrais (*caput*), bem como o que deve ser considerado, para fins da aplicação do MCI, como dados cadastrais.

Em sua redação, o *caput* do art. 9º parece apenas reproduzir o texto do parágrafo 3º do art. 10 do MCI. Porém, traz o acréscimo da "motivação" como um requisito para o pedido de acesso a dados cadastrais por parte de autoridades administrativas competentes. Tal acréscimo, mesmo que positivo para qualificar os pedidos, nos parece contrariar o MCI, pois o parágrafo 3º do art. 10 do MCI, utiliza a expressão "na forma da lei", o que nos leva a concluir que **apenas uma Lei de Proteção de Dados Pessoais poderia definir**.

Além disso, a redação do parágrafo único do art. 9º (que define qualificação pessoal como nome, prenome, estado civil e profissão do usuário) parece **extrapolar o poder normativo de um Decreto**, uma vez que inova em sua definição de qualificação pessoal, algo que na redação do parágrafo 3º do art. 10º do MCI só poderia ser feito por Lei específica.

Recomendação 3: Exclusão do art. 9º por completo da minuta do Decreto por extrapolar o poder normativo do Decreto, uma vez que contraria disposição expressa do §3º do art. 10º do MCI.

Sem dúvida, o dispositivo que nos despertou maior perplexidade na minuta proposta foi o art. 12 em toda sua extensão. Isto porque parece muito claro que o inciso III do art. 3º do MCI exige que a disciplina da proteção de dados pessoais no Brasil seja realizada por Lei e não por regulamento.

[9] BANDEIRA DE MELLO, Celso Antônio. Curso de Direito Administrativo. 32ª edição revista e atualizada até a Emenda Constitucional 84, de 2.12.2014. São Paulo: Malheiros Editores, 2015, p. 351.

Além disso, definir dado pessoal e tratamento de dados sem definições complementares como dados sensíveis, dados anonimizados, titularidade de dados, consentimento, operador, banco de dados, dentre outros, é, no mínimo uma irresponsabilidade. Após meses de debate público sobre a minuta proposta pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais, trazer o tema a partir das definições propostas no art. 12 não atenta para a seriedade que o tema merece.

Pelo texto expresso do inciso III do art. 3º do MCI e pelos esforços empregados no debate público sobre proteção de dados pessoais, corporificado nas contribuições ao Anteprojeto de Lei de Proteção de Dados Pessoais em 2015, esperávamos que as definições de dados pessoais, bem como de tratamento de dados fossem objeto desta Lei, complementando o texto do MCI.

De todo modo, além de reconhecer que **o art. 12 extrapola o poder normativo de um Decreto ao definir dado pessoal e tratamento de dados pessoais**, dedicamos a seção 5 desta contribuição para analisar o conceito proposto, que, em nossa visão, encontra-se anacrônico em relação aos debates recentes sobre o tema e em relação ao texto proposto no Anteprojeto de Proteção de Dados Pessoais apresentado pelo Ministério da Justiça em 2015.

Recomendação 4: Exclusão do art. 12 em toda a sua extensão da minuta do Decreto por extrapolar o poder normativo do Decreto, contrariando previsão expressa do inciso III do art. 3º do MCI e por não reconhecer o debate público promovido pelo Ministério da Justiça em 2015 para elaboração da Lei Brasileira de Proteção de Dados Pessoais.

3. Problemas com a Terminologia Utilizada

A escolha do vocabulário preciso na elaboração de uma norma é sempre um desafio para o formulador de políticas públicas. A tarefa envolve a escolha de termos tecnicamente precisos e claros aos intérpretes. Em particular, a confecção de um regulamento impõe um desafio adicional, a compatibilização do vocabulário escolhido com o texto da Lei a qual se busca regulamentar.

A minuta de Decreto proposta, mesmo incorporando boa parte da terminologia presente no MCI, ainda apresenta dois problemas importantes:

(i) não é precisa no uso de determinados termos, o que a torna obscura para seu intérprete, valendo-se de expressões vagas; e

(ii) algumas passagens não se mostram compatíveis com a terminologia do MCI, em especial ao tratar *dado* e *registro* como sinônimos.

A primeira expressão curiosa disposta no texto da minuta é a de 'serviço especializado' prevista no parágrafo único, inciso II, do art. 2. Não fica claro no texto da minuta se a expressão 'serviço especializado' refere-se a uma das *submodalidades* de Serviço Limitado Privado (SLP), ou Serviço Limitado Especializado (SLE), de competência regulatória da Agência Nacional de Telecomunicações (ANATEL).

Pelo texto do parágrafo único, inciso II, do art. 2º **não fica claro que tipo de serviço está sendo excluído da regulamentação da minuta de Decreto,** uma vez que o inciso I do mesmo parágrafo único já estabelece que serviços de telecomunicações, com exceção do provimento de conexão, serão excluídos da norma. Contudo, **a falta de precisão no uso da expressão 'serviços especializados' dificulta o entendimento do sentido do comando normativo**.

Se a intenção do artigo do inciso II é diferenciar e criar uma categoria de serviços que não será objeto da regulamentação proposta pelo Decreto, bastaria a enumeração dos serviços especializados que não seriam objeto do Decreto regulamentador.

Recomendação 1: Alterar o parágrafo único, inciso II, do art. 2º da minuta de Decreto, criando uma lista de serviços especializados que estarão excluídos da regulação do Decreto.

Recomendação 2: Alternativamente, caso a expressão 'serviço especializado' seja sinônimo de Serviço Limitado Especializado (SLE), recomenda-se a adoção do termo por completo, sem qualquer omissão.

No mesmo sentido, o *caput* do art. 9º da minuta emprega a expressão 'competência' em referência ao parágrafo 3º do art. 10 do MCI. Contudo, o uso da expressão no texto do *caput* do art. 9º traz mais dúvidas do que orientação para sua aplicação.

Em boa medida, o *caput* do art. 9º repete a previsão do §3º do art. 10 do MCI, inovando no acréscimo do requisito 'motivação' para os pedidos de acesso a dados cadastrais. Esperava-

se que o dispositivo regulamentasse qual tipo de competência legal, geral (e.g. fiscalizar determinado setor) ou específica (e.g. capacidade de obter determinado dado cadastral), seria necessária para os pedidos realizados por autoridades administrativas.

Recomendação 3: O *caput* do art. 9º da minuta de Decreto deve esclarecer o sentido da competência legal (geral ou específica) que está disposta no §3º do art. 10 do MCI, de modo a deixar claro qual o requisito formal para solicitação de dados cadastrais segundo o MCI.

Os artigos 10 (incisos II e III) e 11 (*caput*) da minuta de Decreto utilizam a expressão '*provedor de acesso a aplicações*' em alusão ao termo provedor de aplicações de internet na linguagem empregada pelo MCI em diversos artigos (e.g. art. 15, art. 19, art. 20, art. 21, etc.). Curiosamente, o art. 14, *caput*, da minuta emprega outra expressão em alusão a provedores de aplicações de internet, o '*provedor de aplicação*'.

Ressaltamos que **o uso da terminologia do MCI não é apenas um preciosismo linguístico, mas sim uma sinalização clara de que os textos são compatíveis**. O art. 5º do MCI empreende um esforço na diferenciação entre aplicações de internet (inciso VII), como "[...] o conjunto de funcionalidade que podem ser acessadas por meio de um terminar conectado à internet," de registros de acesso a aplicações de internet (inciso VII), como "[...] o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

Fica claro pelas definições do art. 5º do MCI que quando se trata de aplicações, a referência são funcionalidades disponíveis ao usuário, e quando se trata de registros de acesso a aplicações, a referência são informações específicas, data e hora, do acesso à aplicação.

Nesse sentido, **o emprego da expressão 'provedor de acesso à aplicação' mostra-se incompatível com o texto do MCI** pela diferença entre os significados de aplicações de internet e de acesso a aplicações. A manutenção da expressão, conforme apresentada na minuta, pode confundir o intérprete do texto, levando a conclusões equivocadas sobre sua aplicação.

Recomendação 4: Substituir as expressões "provedor de acesso a aplicações", presente nos artigos 10 (incisos II e III) e 11 (*caput*), e "provedor de aplicação", presente no art. 14 (*caput*), pelo termo provedor de aplicações de internet, em consonância com o texto do MCI.

Por fim, o mais preocupante equívoco terminológico presente na minuta do Decreto encontra-se no art. 11. Os incisos II e IV parecem empregar "registro" no mesmo sentido de "dado", **conceitos absolutamente distintos no texto do MCI e no debate de proteção de dados pessoais.**

O inciso II, por exemplo, traz a expressão "tratamento dos registros" em clara referencia a operações de tratamento de dados. O inciso IV, por sua vez, usa a expressão "gestão de registros" por tecnologias de criptografia ou medidas equivalentes. Curiosamente, o inciso V do mesmo artigo utiliza-se da terminologia correta, "tratamento de dados".

Para Rob Kitchin (2014, Kindle Edition), dados são comumente compreendidos como o material bruto produzido por abstrações do mundo em categorias, medidas e outras formas

de representação – números, características, símbolos, imagens, sons, ondas eletromagnéticas, bits – que constituem a fundação na qual informação e conhecimento são criados.

Segundo o autor (2014, Kindle Edition), dados podem ser representados de diversas formas:

(i) natureza, medidas de um fenômeno, como a idade, altura, peso, cor, pressão sanguínea, opinião, hábitos, localização de uma pessoa, etc.;

(ii) presença, por meio da sua presença ou ausência em determinados contexto;

(iii) agregação, podem ser construídos dentro de outros conjuntos;

(iv) derivação, produção a partir de outros dados, como porcentagem de mudança ao longo do tempo calculada ao comparar dados de dois períodos de tempo; e

(v) forma de gravação, analógica ou codificados em forma digital como *bits* (dígitos binários).

Nesse sentido, um registro de conexão ou de aplicação é uma espécie de dado. Isso fica muito claro nas definições dos incisos VI e VIII do art. 5º do MCI, que explicitam os conceitos de registro de conexão e registros de acesso a aplicações de internet.

O inciso VI do art. 5º do MCI define registro de conexão como o conjunto de informações referentes a data e hora de início e término de uma conexão, sua duração e endereço IP utilizado pelo terminal. No mesmo sentido, o inciso VIII do mesmo artigo define registro de acesso a aplicações de internet, substituindo conexão por aplicação de internet.

Portanto, **registro não é qualquer tipo de dado, mas sim uma modalidade de dados específica**. Para os fins do texto do MCI, registro de acesso é o conjunto de informações referentes a data, hora de início e término de uma conexão ou aplicação, sua duração e endereço IP utilizado pelo terminal.

Os incisos II, IV do art. 11 da minuta parecem equivocar-se ao empregar as expressões "tratamento de registros", "acesso aos registros" (inciso II) e "gestão dos registros" (inciso IV) como sinônimo de dados em geral. **Não parece que o sentido de registro atribuído aos incisos da minuta seja o mesmo sentido de registro disposto no MCI.**

Além disso, Rob Kitchin (2014, Kindle Edition) ressalta que vivemos em uma nova economia baseada em dados, em que cada vez mais setores econômicos e sociais estruturam a sua atuação na análise de dados. Compreender o mundo que vivemos hoje passa pelo estudo das transformações nos mecanismos de coleta, análise e acesso a dados. Esta transformação é central a inovações tecnológicas, novas estratégias de comunicação no campo político, expansão das fronteiras do conhecimento científico, dentre outras funções.

Recomendação 5: Substituir a palavra "registro" por "dado" nos incisos II e IV do art. 11 da minuta de Decreto, de modo a evitar equívocos na aplicação da norma.

4. Percepções conflitantes sobre tratamento e gestão de dados pessoais

A Seção II (Padrões de Segurança e Sigilo dos Registros, Dados Pessoais e Comunicações Privadas) da minuta sob análise trata da definição de diretrizes sobre padrões de segurança em operações de guarda, armazenamento e tratamento de dados realizados por provedores de conexão e de aplicação.

O art. 11, em especial, pode ser considerado como a síntese da proposta de regulamentação, ao enumerar quais devem ser os padrões a serem observados por agentes que realizem tais atividades. Contudo, em uma leitura atenta do artigo, notamos que ele **apresenta problemas significativos na forma como concebe operações de tratamento e gestão de dados**, objeto desta seção.

Em síntese, o artigo 11 apresenta os seguintes problemas:

(i) dá um peso grande ao componente humano na gestão e tratamento de dados, quando no cenário atual a maior parte do tratamento e gestão de dados é realizado de forma automatizada; e

(ii) enumera padrões de segurança de forma genérica e pouco precisa, deixando dúvidas relevantes aos agentes do tratamento e gestão de dados pessoais.

Na discussão de proteção à privacidade e padrões de segurança, a proteção à privacidade tem sido marcada por regras que definem quem pode ter acesso aos dados, quais são as responsabilidades para agentes do tratamento de dados, quais são os direitos dos titulares de dados, entre outras. Na definição de padrões de segurança da informação, por sua vez, o escopo de preocupações reside na prevenção ao vazamento de dados, na adoção de medidas contra ataques, dentre outras.

Derek Bambauer (2014, p. 669), por exemplo, diferencia as regras de proteção à privacidade daquelas de garantia da segurança da informação a partir da dicotomia entre controle do acesso legítimo à informação (privacidade) e tecnologias que mediam o acesso ou o controle sobre a informação (segurança).

Nesse sentido, é no mínimo inusitado que em um mesmo artigo (art. 11) o texto proposto na minuta de Decreto busque regular tanto a responsabilidade das pessoas que terão acesso à dados pessoais (inciso I) por meio de um inventário detalhado (inciso III), como também sobre quais as tecnologias a serem adotadas pelos agentes da gestão e do tratamento de dados, tai como mecanismos de autenticação de acessos (inciso II) e tecnologias de criptografia ou medidas equivalentes (inciso IV).

Conforme apontado por Bambauer, há diferenças importantes entre o desenho de uma norma para a proteção da privacidade no contexto de proteção de dados, das regras relacionadas à segurança da informação. A separação dos temas em artigos distintos poderia facilitar a organização do Decreto, de modo a contribuir para sua melhor compreensão e aplicação.

Ademais, há um problema mais grave na redação do art. 11, em particular em seus incisos I e III, quando este utiliza como principal estratégia para a proteção da privacidade o controle

restrito sobre o acesso a dados, com a elaboração de um inventário detalhado dos acessos, e do estabelecimento de privilégios exclusivos e da definição de responsabilidades para as pessoas que realizam a gestão e o tratamento de dados.

Em nossa visão, esses dispositivos refletem uma percepção de gestão e tratamento de dados distante da realidade atual. Atualmente, empresas, entidades de pesquisa e governos cada vez mais *automatizam* suas atividades de coleta, armazenamento, guarda e tratamento de dados. Mesmo que o componente humano ainda seja fundamental para a formulação das atividades e para a sua supervisão, a maior parte da gestão e do tratamento ocorre de forma automatizada, em comunicações máquina a máquina.

Rob Kitchin (2014, Kindle Edition), ao descrever as novas tendências da análise de grandes quantidades de dados (*Big Data*), afirma que o exame de extensivos bancos de dados ou de largas porções de dados só é viável por meio de algoritmos de computador. Mesmo que indivíduos ainda realizem análises de dados ou tomem decisões sob a estrutura de tais algoritmos, a tendência do tratamento de dados é de crescente automatização.

Desta forma, **as disposições presentes nos incisos I e III do art. 11 da minuta – que ressaltam a presença de um componente humano – é no mínimo anacrônica diante da tendência de automação no tratamento de dados**.

Nos preocupa o caminho adotado pela minuta de Decreto, pois o enfoque deveria estar nos contextos em que os dados serão utilizados e nos agentes da gestão e do tratamento de dados (e.g. empresas, governo e entidades de pesquisa), e não nas pessoas que podem estar envolvidas na supervisão de sistemas automatizados.

Recomendação 1: Separar as diretrizes de gestão da privacidade das diretrizes de gestão da segurança da informação em dispositivos normativos distintos.

Recomendação 2: Alterar o enfoque humano da gestão e tratamento de dados presente nos incisos I e III do art. 11 da minuta, para uma abordagem que respeite a tendência de automação destes processos, preservando a responsabilização dos agentes que realizam a gestão e o tratamento de dados.

No tocante aos incisos II, IV e V do art. 11, que estabelecem tecnologias como diretrizes de segurança na gestão e tratamento de dados, há pelo menos dois pontos preocupantes:

(i) a escolha de diretrizes de segurança aplicáveis a todos os mercados; e

(ii) a polissemia de expressões como "criptografia", "medidas de proteção equivalente" e "separação lógica".

Harold Abelson *et al.* (2015, p. 72) apontam para a ampla adoção de técnicas de segurança de dados nas redes globais de comunicação, ressaltando a importância da criptografia como uma das principais tecnologias empregadas neste contexto. Segundo os autores, houve uma mudança na escala e de escopo na adoção de tecnologias de segurança de informação a depender do setor.

Obviamente, mercados como o financeiro e áreas como a saúde terão incentivos em investir em tecnologias mais robustas de segurança da informação, tendo em vista a sensibilidade

destes dados no contexto de suas atividades. Já o mercado de varejo eletrônico, por exemplo, não guarda o mesmo nível de exigência de investimentos para a proteção de dados, podendo adotar tecnologias de segurança menos robustas em termos comparativos.

Para fins de ilustração, vale mencionar a Resolução n.º 1.821/2007 do Conselho Federal de Medicina (CFM) que versa sobre padrões de segurança em sistemas de armazenamento e tratamento de dados dispostos em prontuários médicos. O setor já possui um Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES), editado pelo CFM em conjunto com a Sociedade Brasileira de Informática em Saúde (SBIS), dando conta, em grande medida, dos complexos desafios na gestão de dados pelo setor.

Hoje, a SIBIS conduz a certificação de sistemas no campo da medicina para verificar o atendimento a padrões de segurança definidos pelo setor. Ao contrário do texto proposto pela minuta de Decreto, o Manual de Certificação dispõe de uma **estrutura técnica clara e critérios detalhados** para a gestão de dados de prontuários médicos.

Sendo assim, a escolha da tecnologia de segurança da informação deve estar ligada a características de um mercado específico e à sensibilidade da informação que está sendo gerida ou tratada. **Definir padrões de segurança a partir da enumeração de algumas tecnologias, como notado nos incisos II, IV e V é, em nossa visão, uma estratégia equivocada diante das diferentes exigências de cada setor**.

Ademais, a minuta – ao trazer no inciso IV a expressão "criptografia ou medidas de proteção equivalentes" – não ofereceu critérios ao intérprete sobre o que poderia ser considerado como equivalente. Medidas de proteção equivalentes seriam aquelas tecnologias de segurança da informação restritas ao universo da criptografia ou qualquer técnica de segurança, tais como *firewall*, ofuscamento de dados, dentre outras?

Aspectos como o tamanho da chave criptográfica, se está estruturada de forma assimétrica ou simétrica, se é válida somente durante um espaço de tempo, entre outros, são fatores que definem a robustez do sistema. Nos parece que o Decreto não deveria dedicar-se a definir um padrão de segurança único, mas sim exigir a adoção de boas práticas pertinentes a cada setor. Veja-se, por exemplo, a adoção de boas práticas de segurança da informação recomendadas pelo CERT.br ou entidades internacionais de certificação de segurança da informação.

Da mesma forma, a separação lógica proposta no inciso V do art. 11 da minuta mostra-se de difícil execução para os agentes da gestão e do tratamento de dados, em particular pelas múltiplas formas de armazenamento e tratamento dos mesmos.

Sobre o tema, Rob Kitchin (2014, Kindle Edition) descreve que bancos de dados NoSQL são tipicamente distribuídos entre várias máquinas. Assim, estes bancos de dados conseguem gerir e tratar um vasto conjunto de dados de forma mais eficiente que alternativas de centralização em uma única máquina.

Nesse sentido, a separação lógica de sistemas de tratamento de dados pode não fazer sentido em um contexto de gestão e tratamento de grandes grupos de dados, além de poder ser questionada como estratégia de segurança eficaz neste tipo de contexto.

Recomendação 3: Substituir as diretrizes sobre padrões de segurança dispostas nos incisos II, IV e V do art. 11 pela recomendação de adoção de boas prática de segurança pertinentes ao setor de atuação de cada agente que promove a gestão e tratamento de dados.

Por fim, é necessário comentar os dispositivos presentes nos artigos 13 e 14 da minuta do Decreto. São dois os problemas pertinentes a estes artigos:

(i) a possível confusão entre facilitação de acesso e a criação de um *backdoor* na redação do art. 13; e

(ii) o grau de detalhamento das informações sobre padrões de segurança a serem publicados por provedores de conexão e aplicação de internet, conforme a redação do art. 14.

O *caput* do art. 13 da minuta de Decreto, em cumprimento ao art. 10 do MCI, estabelece o dever de adoção de formatos que facilitem o acesso a dados decorrentes de decisão judicial ou determinação legal por parte de provedores de conexão e de aplicações de internet. Contudo, **o artigo não esclarece nada mais sobre qual seria este formato**, o que nos leva a questionar se não **estaria o artigo referindo-se à criação de um canal remoto e exclusivo de acesso a dados (*backdoor*) para autoridades públicas?**

Pelas disposições do MCI, o dever de guarda de registros (artigos 13 e 15), bem como o dever de disponibilizá-los mediante ordem judicial (§3º do art. 10 e art. 22) estão se consolidando no dia a dia do setor. Todavia, não há no texto do MCI nenhuma previsão ou indicação que assegure ao Poder Público o direito de constituir um canal exclusivo para o acesso aos dados, mesmo que tenha sido expedida uma ordem judicial para tanto.

A falta de clareza do dispositivo nos faz questionar inclusive a relação entre privacidade e segurança proposta na minuta. A criação de uma *Backdoor* por Decreto, sem uma ampla discussão na sociedade, e sem uma definição de quais os limites para o uso dos dados coletados, mostra-se um perigo direto e real para a proteção da privacidade no Brasil.

Além disso, a criação de uma *backdoor*, a depender de sua estrutura técnica, pode vir a representar um risco de segurança para os dados, uma vez que o canal de acesso remoto também poderá ser utilizado por aqueles que pretendem realizar ataques a infraestruturas sensíveis para obter dados de usuários.

A título de ilustração, vale mencionar a nossa preocupação com a possibilidade de exigência de *backdoors* em sistemas de criptografia, uma vez que é corrente a avaliação de que a criação de acessos facilitados em criptografia em muitos casos resulta no enfraquecimento da ferramenta como um todo (ABELSON, Harold et al., 2015; GASSER, Urs et al., 2016).

Em nossa visão, este é um debate que não está maduro, não existindo ainda soluções razoáveis nos Estados Unidos da América, na Europa e na Ásia. Não recomendamos, assim, a inserção do dispositivo da forma como ele se encontra.

Recomendação 4: Exclusão do art. 13 da minuta de Decreto do MCI.

Por fim, o *caput* do art. 14 da minuta de Decreto cria o dever de divulgação de informações sobre padrões de segurança adotados por provedores de conexão e aplicação na internet. Todavia, a norma não estabelece qual o grau de detalhe da informação será necessário para o seu cumprimento.

Provedores de serviços no mesmo segmento podem divulgar informações muito diferentes entre si sobre seus padrões de segurança sem qualquer prejuízo para a clareza e acessibilidade da informação. É muito diferente a divulgação da informação de que a Empresa X adota criptografia como padrão de segurança, para a Empresa Y que adota criptografia assimétrica dispondo de uma dupla chave privada. Hoje, pela redação do art. 14, não está clara qual a orientação os provedores de serviços na internet devem seguir para adequarem-se ao texto da norma.

Além disso, uma disponibilização pública e detalhada de padrões de segurança poderia também representar um risco à própria segurança da informação. Uma descrição de todas as medidas adotadas pode servir de orientação para aqueles que almejam, por exemplo, invadir determinado sistema eletrônico.

Nesse sentido, acreditamos que a divulgação de padrões de segurança deve ser genérica, sempre respeitando as boas práticas de segurança de cada setor da economia.

Recomendação 5: As informações solicitadas no art. 14 devem ter caráter geral e não específico, sinalizando para os usuários de serviços que seus dados estão protegidos, sem contudo, relevar no detalhe informações relevantes sobre o padrão de segurança adotado.

5. A importância do conceito de dado pessoal

Entre todos os pontos de nossa contribuição, dedicamos um espaço privilegiado para discutir a proposta de conceito de dado pessoal inscrita na minuta do Decreto. Esta proposta nos preocupa em três aspectos:

(i) foi oferecida no contexto de uma minuta de Decreto regulamentador, diploma normativo claramente inadequado para tal propósito;

(ii) não reconhece a importância do conceito de dado pessoal como a "espinha dorsal" de um modelo jurídico de proteção de dados pessoais; e

(iii) o conceito sugerido na minuta mostra-se anacrônico em relação ao debate atual sobre proteção de dados no Brasil e no mundo, em especial se comparado com o conceito proposto no Anteprojeto de Proteção de Dados Pessoais do Ministério da Justiça.

Tendo em vista que já discutimos a inadequação da proposta de um conceito de dado pessoal frente à previsão expressa do inciso III do art. 3º do MCI na seção 2 desta contribuição, trataremos nesta seção dos problemas intrínsecos ao conceito de dado pessoal proposto na minuta de Decreto.

Porém, vale reforçar a nossa surpresa com a **falta de cuidado no tratamento do tema**, tendo em vista o amplo debate público sobre a definição de dado pessoal realizada no contexto do Anteprojeto de Proteção de Dados Pessoais conduzido pelo Ministério da Justiça. Toda evolução na construção do texto do Anteprojeto de Proteção de Dados Pessoais resultante da participação pública sobre o texto, em especial no aprimoramento do conceito de dado pessoal, parece ter sido ignorada pela minuta do Decreto.

Por esta razão, acreditamos que valha a pena explicar qual a posição do conceito na regulação da proteção de dados.

Paul M. Schwartz e Daniel J. Solove (2014, p. 1) apontam que a aplicação de Leis e regulamentos de proteção de dados e de defesa da privacidade guarda uma relação de dependência direta com a definição de dado pessoal. Isto porque, a depender da definição atribuída, reduz-se ou amplia-se o conjunto de agentes participantes da cadeia de coleta, armazenamento e tratamento de dados e o grau de sua responsabilidade frente à gestão destes dados.

A definição de dado pessoal confere a qualquer modelo regulatório de proteção de dados uma moldura de possibilidades normativas para a legislador e para os formuladores de políticas públicas. É a partir deste conceito que se pode definir titularidade de dados, agentes da gestão de dados, consentimento, anonimização, limites para a transferência internacional de dados, acesso por autoridades administrativas, dentre outros.

Os autores (2014, p. 2) apontam que a fragmentação em diplomas normativos distintos nos Estados Unidos da América tem representado um entrave à efetiva proteção de dados pessoais naquele país. Nos Estados Unidos, há três definições distintas para dado pessoal que

variam por setor regulado, criando um cenário no qual o mesmo dado pode ser objeto de proteção ou não, a depender daquele que o detém.

A título de ilustração, os autores mencionam dois exemplos. O *Video Privacy Protection Act* de 1988 define dado pessoal como aquela informação capaz de identificar uma pessoa (*personally identifiable information*). O *Gramm-Leach-Bliley Act* de 1999, por sua vez, define dado pessoal no mercado financeiro como informação pessoal não-pública (*nonpublic personal information*). No limite, um vídeo dentro de uma instituição financeira transmitido ao vivo e sem restrições na internet receberia a proteção conferida à dados pessoais?

Recomendação 1: Não definir dado pessoal sem o acompanhamento de um regime de proteção de dados pessoais que estabeleça como e qual dado está protegido, pois a definição serve como moldura normativa para o regime.

Recomendação 2: Não fragmentar o regime jurídico de proteção de dados pessoais com a definição de dado pessoal em mais de um diploma normativo. O local para a definição de dado pessoal é a futura Lei de Proteção de Dados Pessoais.

A União Europeia evitou o problema estadunidense da fragmentação do conceito de dado pessoal pela edição da Diretiva n.º 46/95 EC. Segundo o *Handbook on European data protection law*[10] (2014, p. 18) a intenção do diploma normativo era harmonizar legislações nacionais de proteção de dados de seus membros, garantindo que os países seguissem um mesmo padrão.

Todavia, Schwartz e Solove (2014, p. 2) apontam que a tradicional definição de dado pessoal como a informação que identifica ou que é capaz de identificar uma pessoa natural, criada em 1995 pela alínea a do art. 2º da Diretiva n.º 46/95, tem sofrido críticas importantes, capazes de convencer a entidade a iniciar debates para reformar a Diretiva 46/95 a partir de uma nova proposta regulatória[11].

[10] O *Handbook on European data protection law* é uma publicação de 2014 da *European Union Agency for Fundamental Rights* em conjunto com a *European Court of Human Rights e o Conseil de L'Europe*. A publicação é um esforço de autoridades europeias em esclarecer a aplicação da Diretiva n.º 46/95 no contexto dos casos julgados pela Corte Europeia de Direitos Humanos. Este é o documento que serve de orientação para juristas que atuam na área de proteção de dados na Europa ocidental. Está disponível em: < http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Acesso em 14.02.2016.

[11] A nova proposta de reforma do regime jurídico de proteção de dados pessoais da União Europeia toma o cuidado de explicar o contexto da proposta de alteração da Diretiva n.º 46/95, explicando o amplo processo de consulta pública as partes afetadas pela regulação, bem como explicando a estrutura jurídica da proposta, extrapolando o texto normativo proposto. Ela está disponível para consulta em: < http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>. Acesso em: 12.02.2016.

O principal problema apontado para o conceito de dado pessoal, tal qual definido no texto da Diretiva n.º 46/95[12], semelhante ao proposto na minuta de Decreto[13] de regulamentação do MCI, reside na dificuldade em se separar dados protegidos e, portanto, dignos de cuidados especiais, daqueles dados que não necessitam de tal proteção.

O conceito de dado pessoal como o dado relacionado à pessoa natural identificável, no limite, pode tratar de todo e qualquer dado, pois qualquer dado pode ter em algum momento relação com uma pessoa natural.

O uso do termo *identificável* sem qualquer limite para a associação do dado em relação à pessoa pode criar cenários em que qualquer dado seja digno de proteção jurídica, fato que pode prejudicar um conjunto de atividades desde pesquisas acadêmicas à novos negócios.

Um exemplo disso é o número do endereço IP (Internet Protocol). Conforme define o inciso III do artigo 5º do MCI, o endereço de protocolo de internet é "o código atribuído a um terminal de uma rede para permitir sua identificação, definindo segundo parâmetros internacionais;". A definição não trata que este número, um dado, necessariamente seja relacionado a uma pessoa natural ou mais pessoas, uma vez que é atribuído a um terminal. Nesse sentido, o número IP pode ser um dado que *em determinado contexto* pode referir-se à conexão de um terminal, utilizado por múltiplas pessoas.

Durante as atividades de pesquisa do GEPI, por exemplo, é muito comum que os pesquisadores se utilizem dos mesmos terminais com privilégios de navegação de bancos de dados de artigos científicos internacionais na biblioteca Karl A. Boedecker em uma mesma tarde, ou seja, com o mesmo número IP.

Pode-se dizer que o número atribuído para esta conexão é capaz de identificar uma pessoa natural, enquadrando-se na definição do inciso I do art. 12 da minuta de Decreto? Sem dúvida. Contudo, faz sentido que este dado seja considerado como um dado pessoal neste contexto? Em nossa visão, não. Não há uma relação direta entre dado e indivíduo, uma vez que o número em si será o mesmo durante todo o período de uso do terminal.

Desde 1995, a União Europeia e a Corte Europeia de Direitos Humanos têm buscado dar sentido à expressão 'identificável' presente no conceito de dado pessoal de sua Diretiva. O *Article 29 Data Protection Working Party*, por exemplo, publicou, em 2007, um estudo[14] sobre o conceito de dado pessoal, no qual busca esclarecer como o conceito de informação identificável tem sido utilizado no contexto europeu.

---

[12] Nas palavras da Diretiva n.º 46/95 da União Europeia: "*Article 2 – Definitions - For the purposes of this Directive: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*"

[13] No texto da minuta: "Art. 12. Para os fins do disposto neste Decreto, considera-se: I- dado pessoal como dado relacionado à pessoal natural identificada ou identificável, inclusive a partir de números identificadores, dados locacionais ou identificadores eletrônicos, compreendendo inclusive registros de conexão e acesso a aplicações e conteúdo de comunicações privadas;".

[14] UNIÃO EUROPEIA, Parlamento Europeu, *The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data*. Opinion 4/2007 on the concept of personal data. Acesso em: 20/02/2016. Disponível em: < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>

Diferente do inciso I do art. 12 da minuta de Decreto, o *Recital 26* da Diretiva 46/95 esclarece que para a verificar se uma informação é capaz de identificar uma pessoa é necessário que se leve em consideração todos os meios que foram usados para a identificação por todos os evolvidos no processo de coleta e tratamento dos dados.

Na visão do *Article 29 Data Protection Working Party* (2007, p. 15) a mera possibilidade de identificação em abstrato, hipotética, inerente a uma associação remota entre dado e indivíduo, não deve ser considerada como dado pessoal para fins da aplicação da Diretiva 46/95. O estudo ilustra esta ideia a partir de exemplo útil para sua melhor compreensão.

Nas pesquisas para o desenvolvimento de novos medicamentos, equipes de pesquisa médica lidam com grandes quantidades de dados capazes de identificar indivíduos em situação de tratamento de doenças, em testes experimentais de novas drogas para o combate de doenças, dentre outros cenários. Nessas situações, o protocolo adotado pelas equipes de pesquisa é o de substituir o nome destes pacientes por números, atribuídos aleatoriamente para cada um dos casos.

Para evitar confusões e para um melhor aproveitamento estatísticos dos dados, os números seguem uma lógica seriada, com identificadores capazes de atribuir sentido para cada teste realizado. Os nomes dos pacientes associados aos dados da pesquisa permanecerão confidenciais, em posse dos médicos que os atenderam. Estes médicos, ao compartilharem informações com equipes de pesquisa, irão sempre omitir o nome do paciente, já que seria o principal elemento de identificação pessoal.

No contexto europeu, estes dados utilizados no exemplo citado acima não seriam considerados dados pessoais, pois mesmo que remotamente identificáveis, os meios empregados pelos médicos em conjunto com a equipe de pesquisa para anonimização dos dados são considerados como suficientes para desassociar o dado da identidade individual.

Como consequência, os dados obtidos de pacientes europeus para fins da pesquisa não necessitariam do consentimento individual de cada um dos pacientes para serem utilizados. A pesquisa ganharia em termos quantitativos e qualitativos e informações sensíveis não poderiam ser associadas a pessoas naturais.

Todavia, pela redação atual do inciso I do art. 12 da minuta de Decreto, as informações anonimizadas do exemplo trazido seriam consideradas dados pessoais, uma vez que não há nenhuma ressalva ou limite no texto da norma que exija uma relação direta entre dado e pessoa.

Neste tópico, queremos reforçar que o Anteprojeto de Proteção de Dados Pessoais proposto pelo Ministério da Justiça, alinhado com a nova proposta de regulação europeia, propõe um conceito mais sofisticado para dado pessoal, orientado a capacidade de associação do dado à pessoa em determinados contextos.

Nas palavras do art. 5º, inciso I da última redação do Anteprojeto de Proteção de Dados Pessoais:

> "Art. 5º Para os fins desta Lei, considera-se:

> I – dado pessoal: dado relacionado à pessoa natural identificada ou indentificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;" (grifo nosso)

A redação do inciso I oferece um conceito que trata o dado pessoal como uma condição relativa a um determinado contexto, e não uma característica inerente ao dado em si. Esta diferença é fundamental para o tratamento de dados anonimizados, uma vez que muito se discute sobre a possibilidade destes dados serem considerado como dados pessoais.

Pela definição proposta pela minuta de Decreto, dados coletados de uma pessoa natural, ainda que posteriormente anonimizados, poderiam ser considerados dados pessoais em si, mesmo em contextos em que a sua associação com o individuo objeto da coleta inicial seja remota.

Na definição do Anteprojeto, os dados anonimizados não seriam por si só considerados como dados pessoais. Em última instância, dependem do seu contexto, podendo estar associados a outros dados, para serem considerados como dados pessoais ou não.

Isto não significa que dados anonimizados estarão sempre excluídos da condição de dado pessoal; ao contrário, **significa que será o contexto que irá conferir a característica de pessoalidade ao dado.**

A este respeito, recomendamos a leitura do estudo elaborado pelo *Article 29 Data Protection Working Party* em 2014 sobre a efetividade de sete diferentes técnicas[15] de anonimização de dados. A pesquisa busca compreender qual a capacidade das principais técnicas de anonimização em dissociar dados da identidade de seus titulares.

Recomendação 3: Abandonar o conceito de dado pessoal presente no Decreto e empregar esforços na aprovação de uma Lei de Proteção de Dados Pessoais com os atributos do Anteprojeto de Proteção de Dados Pessoais elaborado pelo Ministério da Justiça, e amplamente discutido pelos setores interessados.

[15] As sete técnicas analisadas pelo estudo foram: (i) *Noise Addition*, (ii) *Permutation*, (iii) *Differential Privacy*, (iv) *Aggregation*, (v) *K-Anonymity*, (vi) *L-Diversity*, e (vii) *T-Closeness*. Na análise de robustez de cada técnica, foram utilizadas três perguntas: É possível singularizar um indivíduo? É possível conectar registros de dados a um indivíduo? É possível inferir informações a respeito de um indivíduo? Para verificar os resultados do estudo, consulte: <http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf>.

Referências

ABELSON, Harold *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, v. 1, n. 1, 2015, p. 69-79.

BAMBAUER, Derek E. Privacy Versus Security. *The Journal of Criminal Law & Criminology*. v. 103, n. 3, 2013, p. 667-684.

BANDEIRA DE MELLO, Celso Antônio. *Curso de Direito Administrativo*. 32ª edição revista e atualizada até a Emenda Constitutcional 84, de 2.12.2014. São Paulo: Malheiros Editores, 2015.

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. Vigésima Sétima Edição. São Paulo: Atlas, 2013.

GASSER, Urs *et al.* Don't Panic. Making Progress on the "Going Dark" Debate. The Berkman for Internet & Society at Harvard University, 2016. Acesso em: 20/02/2015. Disponível em: <https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>.

KITCHIN, Rob. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. Los Angeles: SAGE Publications, 2014, Kindle Edition.

LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de Internet. **Revista Jus Navigandi**, Teresina, ano 15, n. 2592, 6 ago. 2010. Disponível em: <https://jus.com.br/artigos/17128>. Acesso em: 21 fev. 2016.

MEDAUAR, Odete. *Direito Administrativo Moderno*. 18ª edição revista e atualizada. São Paulo: Revista dos Tribunais, 2014.

MEIRELLES, Hely Lopes. *Direito Administrativo Brasileiro*. 41ª edição, atualizada até a Emenda Constitucional 84, de 2.12.2014. São Paulo Malheiros Editores, 2015.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. Defining 'Personal Data' in the European Union and U.S.. *Bloomberg BNA Privacy and Security Law Report*. Acesso em: 10/02/2016. Disponível em: <http://docs.law.gwu.edu/facweb/dsolove/files/BNA-Schwartz-Solove-PII-US-EU-FINAL.pdf>.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, v. 86, 2011, p. 1814-1894.

SWIRE, Peter; AHMAD, Kenesa. Encryption and Globalization. *The Columbia Science Technology Law Review*. V. 13, 2012, p. 416-481.

UNIÃO EUROPEIA, Conselho Europeu, European Union Agency for Fundamental Rights. *Handbook on European data protection law*. Luxemburgo: Publications Office of the European Union, 2014.

UNIÃO EUROPEIA, Parlamento Europeu, The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. *Opinion 04/2007 on the concept of personal data*. Acesso em: 20/02/2016. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>.

UNIÃO EUROPEIA, Parlamento Europeu, The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. *Opinion 05/2014 on Anonymisation Techniques*. Acesso em: 20/02/2016. Disponível em: <http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf>.