ISSN xxx-xxxx

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

DADOS PESSOAIS E DADOS SENSÍVEIS: A INSUFICIÊNCIA DA CATEGORIZAÇÃO

Guilherme Damasio Goulart[1]

RESUMO

O presente artigo tem o objetivo de abordar os conceitos de dados pessoais e dados sensíveis levando em consideração os danos causados ao sujeito quando da sua violação. A doutrina defende, em geral, que os dados sensíveis são aqueles que, além de refletirem aspectos mais íntimos do indivíduo, também têm um potencial de causarem danos mais intensos em situações em que há seu mau uso. Propõe-se, a partir disso, que dependendo do contexto, o mau uso de dados pessoais não sensíveis também pode causar danos de maior intensidade ao sujeito.

Palavras-chave: dados pessoais; dados sensíveis; responsabilidade.

INTRODUÇÃO

Tradicionalmente, faz-se uma divisão dos tipos de dados pessoais baseando-se no critério da sensibilidade. Há, assim, os dados pessoais propriamente ditos que trazem elementos que identificam (ou podem identificar) uma pessoa. Há, por outro lado, os dados sensíveis que, além de identificarem a pessoa, revelam elementos mais profundos de sua personalidade, como sua posição política, ideológica, religiosa, sexual, além de trazerem, entre outros aspectos, informações relacionadas à saúde, origem racial, étnica e genética[i].

Nota-se, diante dessa breve definição, que todos os dados sensíveis são dados pessoais, mas o contrário não pode ser dito. Afirma-se, também, que a violação de dados sensíveis é muito mais prejudicial para a pessoa em causa, podendo gerar danos mais intensos à sua personalidade. Outra abordagem envolve a consideração de que o mau uso de dados sensíveis pode trazer maiores possibilidades de discriminação do indivíduo[ii].

A questão que se coloca, a partir disso, é sobre a possibilidade de que danos mais intensos à personalidade do indivíduo possam ser causados também com o mau uso de dados pessoais e não apenas com mau uso de dados sensíveis.

1 BREVÍSSIMOS ASPECTOS GERAIS DE PROTEÇÃO DE DADOS

[1] Mestre em Direito pela UFRGS. Professor em nível de graduação, do curso de Direito do Cesuca e, em nível de pós-graduação, em diversas outras instituições. Email: guilherme@direitodatecnologia.com.

Os tribunais têm dificuldades em reconhecer o dano pelo mau uso de dados pessoais ou sensíveis[iii]. Em geral, acabam por decidir que a "publicidade"[iv] dos dados pessoais permitiria, por si só, que os dados possam ser utilizados de qualquer maneira pelas empresas[v]. Tal argumento, quando observado sob a ótica dos princípios de proteção de dados pessoais (incluída aí a ideia de autodeterminação informacional), é absolutamente incorreto. A eventual publicidade de um dado pessoal ou sensível não tem o condão de permitir o uso descontrolado dos dados pelas empresas. Um dos princípios aplicáveis a esses casos é o da *finalidade*, que indica que um dado pessoal ou sensível, se recolhido para determinada finalidade, não pode ser utilizado para outra[vi]. Igualmente, a finalidade do tratamento de dados não deve ser ilícita nem prejudicar os titulares dos dados. Assim, mesmo dados públicos não são livres para serem utilizados com qualquer finalidade[vii].

A dificuldade dos tribunais reconhecerem a questão do dano envolvendo o mau uso de dados pessoais, contudo, parece estar mudando. Uma sentença da 16ª Vara Cível de Porto Alegre, em sede de Ação Coletiva, considerou ilícita a atividade de venda de informações cadastrais (e pessoais, por consequência) pelo SPC Brasil sem a anuência prévia dos sujeitos[viii]. O assunto é complexo e, em função do espaço, não pode ser tratado em sua completude. Mesmo assim, é necessário afirmar que o tema deve ser abordado levando em consideração o diálogo com o Código de Defesa do Consumidor, a Lei do Cadastro Positivo[ix] e também o Marco Civil da Internet[x], visto que tais serviços são oferecidos via Internet.

Alguns aspectos da disciplina de proteção de dados devem ser invocados para a explicação da licitude ou ilicitude de tais atividades. Um ponto importantíssimo desta disciplina é a consideração da chamada *autodeterminação informacional*[xi], que envolve a possibilidade do sujeito decidir como os seus dados serão tratados[xii]. É justamente a consideração deste princípio que indica que as empresas não podem fazer o que bem entenderem com os dados pessoais, mesmo que eles sejam de acesso público irrestrito, ou seja, estejam publicados na internet. O mesmo princípio traz também em si o dever das empresas informarem os sujeitos de que seus dados estão sendo tratados[xiii], o que também é conhecido como princípio da *transparência*[xiv]. A necessidade de transparência da atividade de coleta e tratamento é um aspecto crítico visto que, atualmente, é muito difícil para o cidadão saber quem possui suas informações[xv].

2 A INSUFICIÊNCIA DA CATEGORIZAÇÃO DE DADOS PESSOAIS

Tendo em vista a referida diferenciação e a brevíssima explanação de alguns princípios de proteção de dados, é necessário dizer que a simples divisão em duas categorias pode não ser suficiente para tratar de situações mais específicas.

Há a necessidade de se contextualizar a situação concreta pois um dado pessoal (não sensível), quando colocado em determinado contexto, pode revelar informações sensíveis. Veja-se, por exemplo, o recente caso do site de encontros extraconjugais Ashley Madison. Um grupo de crackers, como anunciado pela imprensa, conseguiu acesso ao banco de dados daquela empresa vazando dados pessoais de seus usuários. Vazou-se, entre outras informações, os endereços de e-mail dos usuários daquela plataforma. Ora, um endereço de e-mail, quando visto isoladamente, é um dado pessoal; seu mau uso isolado não tem o condão de causar grandes danos ao sujeito. Porém, este mesmo e-mail, quando relacionado a um site de encontros extraconjugais, faz com que se descubra um aspecto altamente sensível do sujeito, qual seja, um tipo de comportamento sexual que, no caso do site, o sujeito certamente gostaria de manter em sigilo[xvi].

Isso indica que um dado pessoal (e não sensível) se estiver relacionado a um contexto específico pode causar grandes danos ao sujeito. Neste ambito, diz Helen Nissembaum que há quatro transformações cruciais envolvendo as violações de dados pessoais na atualidade: a democratização das tecnologias de bancos de dados, a mobilidade da informação, a agregação da informação e o conhecimento retirado das informações[xvii].

A referida divisão também fica afetada quando o processamento de dados pessoais faz nascer dados sensíveis. As técnicas de *big data* e *data mining* permitem que, ao se submeter dados desconexos ou que não trazem informações sensíveis a um tratamento estatístico, nasça a possibilidade de revelação de novas informações (estas sensíveis). Na verdade, uma das formas mais comuns de *data mining* é a análise preditiva ou "*predictive data mining*". Tal atividade é composta da exploração inicial de dados com a posterior construção de modelos envolvendo a identificação de padrões[xviii].

CONCLUSÕES

A questão proposta aqui não tem a intenção de afirmar que a divisão entre dados pessoais e dados sensíveis seja inútil. O que este pequeno artigo intenta é demonstrar sua insuficiência para situações em que o tratamento de dados é realizado com a utilização de técnicas de *data mining* ou quando há a mudança do contexto dos dados.

Isso importa em dizer que é possível gerar dados sensíveis a partir de dados não sensíveis - ou seja, a partir de dados pessoais. Tal situação demonstra, portanto, a possibilidade de ocorrência de danos por meio do mau uso de dados ou informações aparentemente inofensivos.

REFERÊNCIAS

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor**, São Paulo, n. 46, abr.-jun./2003

LYON, David. **The Eletronic Eye**: The rise of surveillance society. Minneapolis: University of Minnesota, 1994

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In. MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P.. **Direito, Inovação e Tecnologia**. V. 1. São Paulo: Saraiva, 2015

NISSEMBAUM, Helen. **Privacy in context**: Technology, Policy, and the Integrity of Social Life.Stanford: Stanford University Press, 2010.

SOLOVE, Daniel. **The Digital Person**: Technology and privacy in the information age. New York: New York University Press, 2004.

SU, Chunhua et al. Privacy-Preservation Techniques in Data Mining. In: ACQUISTI, Alessandro et al. **Digital Privacy**: Theory, Technologies, and Practices. New York, Auerbach Publications, 2008.

[i] O assunto é tratado no art. 5º do Anteprojeto de Proteção de Pessoais em seu art. 5º, inc. I (dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos) e III (dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos). É possível ver também o conceito de dado pessoal no art. 4º, inc. IV da Lei de Acesso à Informação (Lei 12.527/2011) e o conceito de dado sensível, ou informação sensível, no art. 3º, §3ª, inc. II da Lei do Cadastro Positivo (lei 12.414/2011). A mesma classificação, com pequenas variações, é usada praticamente em todos os países que regulam a proteção de dados pessoais.

[ii] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 163.

[iii] Cf. é possível ver em: TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 9ª Câmara Cível. Apelação n. 70059732305. Mário José de Oliveira Leal x Procob S.A. Relator: Des.ª Iris Helena Mdeiros Nogueira. Porto Alegre, 11 de Junho de 2014 e TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 9ª Câmara Cível. Apelação n. 70060163623. Cezar Augusto Calegaro x Procob S.A. Relator: Des. Miguel Ângelo da Silva. Porto Alegre, 29 de Abril de 2015.

[iv] Ou seja, o fato de poderem ser encontrados com certa facilidade

[v] Mudança que se percebe com a recente sentença citada anteriormente.

[vi] Ver MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.p. 70. Ao falar sobre o princípio da finalidade ela diz que a atividade de processamento deve respeitar "a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta de dados". O Anteprojeto [de proteção de dados] trata a questão nos inc. I e II do art. 6º, respectivamente, os princípios da finalidade e adequação. O último envolve também "*as legítimas expectativas do titular, de acordo com o contexto do tratamento*".

[vii] Recentemente, muitas pessoas ficaram preocupadas ao conhecerem o site "Tudo Sobre Todos" que disponibiliza uma série de informações pessoais dos brasileiros. O que muitos não sabem é que no Brasil há uma série de outras empresas que realizam a mesma atividade já há muitos anos. Empresas como Serasa Experian e SPC fornecem serviços semelhantes, que envolvem a venda de listas cadastrais pela Internet.

[viii] 16ª Vara Cível de Porto Alegre. Processo n. 001/1.14.0178998-7. Ministério Público X Confederação Nacional de Dirigentes Lojistas. Juiz Sílvio Tadeu de Ávila. J. em 28 de Agosto de 2015.

[ix] Lei 12.414/2011.
[x] Lei 12.965/2014.
[xi] Sobre o tema ver CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor**, São Paulo, n. 46, abr.-jun./2003.
[xii] Tal direito envolve também a capacidade de o sujeito decidir quando seus dados serão recolhidos e por quanto tempo serão processados. Como todo o direito ele não pode ser exercitado de forma ilimitada pelo sujeito e há situações onde, mesmo sem a anuência, os dados de um sujeito podem ser recolhidos e armazenados, como se vê na disciplina dos cadastros restritivos de crédito. Neste caso, mesmo sem a anuência, deve o consumidor ser informado da sua inclusão em tais cadastros.
[xiii] Idem. Ibidem, p. 93. Não se admite que existam bancos de dados secretos ou que as pessoas não saibam que seus dados estejam sendo tratados.
[xiv] Previsto no Anteprojeto de Proteção de Dados Pessoais, no art. 6º, in. VI.
[xv] David Lyon chamava atenção para este fato já em 1994. LYON, David. **The Eletronic Eye**: The rise of surveillance society. Minneapolis: University of Minnesota, 1994, p. 4
[xvi] Não é possível abordar aqui os aspectos morais da intenção da pessoa trair seu parceiro. O que se quer abordar é a necessidade de proteção mais intensa dos dados sensíveis. A jurisprudência alemã já entende que há, inclusive, um direito fundamental à proteção da confidencialidade e integridade dos sistemas eletrônicos. Sobre o tema ver MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In. MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P.. **Direito, Inovação e Tecnologia**. V. 1. São Paulo: Saraiva, 2015.
[xvii] NISSEMBAUM, Helen. **Privacy in context**: Technology, Policy, and the Integrity of Social Life.Stanford: Stanford University Press, 2010, p. 37-45.A autora defende a tese da "integridade contextual", que deve ser aplicada à disciplina de proteção de dados.
[xviii] SU, Chunhua et al. Privacy-Preservation Techniques in Data Mining. In: ACQUISTI, Alessandro et al. **Digital Privacy**: Theory, Technologies, and Practices. New York, Auerbach Publications, 2008, p. 188. Daniel Solove chama essa possibilidade de "aggregation effect", cf. SOLOVE, Daniel. **The Digital Person**: Technology and privacy in the information age. New York: New York University Press, 2004, p. 44.