Representação ao Ministério Público de Minas Gerais - MPMG

1. O **INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS,** pessoa jurídica de direito privado constituída na forma de associação de fins não econômicos e organização da sociedade civil, com sede na Rua dos Guajajaras, nº 40, sala 502, Centro, Belo Horizonte/MG, CEP 30180-000, inscrito no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda sob o número CNPJ/MF 23.333.533/000190, por seus procuradores que esta subscrevem, vem, respeitosamente, perante Vossa Excelência, submeter Representação, com o objetivo de contribuir para a efetivação de maior transparência e solicitar providências no que diz respeito ao uso e proteção de dados pessoais em estabelecimentos farmacêuticos em Belo Horizonte e outras cidades do estado de Minas Gerais.

I. Sobre o Instituto e legitimidade para a Representação

O *Instituto de Referência em Internet e Sociedade* - IRIS, de acordo com seu estatuto consolidado em 28 de abril de 2017, constitui-se como associação civil de cunho científico e formulação de políticas nas áreas direito e tecnologia, internet e inovação. Suas atividades buscam servir como uma plataforma independente de estudos, centrada na articulação entre teoria e prática. O Instituto busca consolidar-se como referência no contexto nacional, cooperando com organizações governamentais, empresariais, da sociedade civil e da academia, no Brasil e exterior, em temas relativos às suas áreas de atuação. Encontram-se, entre os objetivos do Instituto, o desenvolvimento e plena participação em projetos de advocacia pública, com relacionamento em

processos judiciais e extrajudiciais de elevado impacto em questões de interesse público e coletivo, em áreas afins aos temas do IRIS.

II. Dos Fatos

Desde 2017, tem sido prática comum que farmácias de Belo Horizonte e de outras cidades brasileiras solicitem o número do Cadastro Nacional de Pessoas Físicas - CPF dos clientes para realizar qualquer compra em seus estabelecimentos. O fornecimento desse dado de identificação pessoal tem como alegada contraprestação ao consumidor somente a atribuição de descontos sobre produtos que estejam vinculados a uma promoção. Essa prática está sendo adotada pelas mais diversas redes de farmácias, inclusive algumas cujas redes atuam em todo o território nacional.[1]

Nenhuma dessas redes de farmácias demonstra de forma transparente para os consumidores qual seria o propósito efetivo dos estabelecimentos ao coletar e armazenar informações individualizadas sobre o histórico de compras de cada cliente. Como exemplo dessa prática, citamos o programa de descontos da Drogaria Araujo "Tem + Araujo"[2]. A sociedade empresária assim dispõe sobre o armazenamento dos números de CPF[3]:

> **"2. Por que vocês querem meu CPF? Resposta:** Para registro no sistema, possibilitando vantagens no Tem + Araujo, novo programa de relacionamento e descontos como nos kits do tabloide.

[1] MARCHETTI, Bruno. *A distopia do 'me fala o CPF' nas farmácias do Brasil*. Revista Vice. Publicado em 15 de fevereiro de 2018. Disponível em: <https://www.vice.com/pt_br/article/9kzbx5/por-que-farmacias-insistem-para-ter-seu-cpf>

[2] Ressalta-se que outras empresas e drogarias tais como Carrefour., possuem práticas comerciais semelhantes envolvendo programas de descontos em troca de dados pessoais de seus consumidores.

[3] Ver mais em: http://blog.Araujo.com.br/acontece-na-Araujo/chegou-o-tem-Araujo-vantagens-pra-voce-que-e-de-casa/

> **3. É seguro informar o CPF para o programa? E a minha privacidade? Resposta:** No sistema da Araujo, o CPF é transformado em um código interno e nenhum funcionário Araujo ou terceiro tem acesso aos dados do cliente ou às suas informações de compras.
>
> **4. Tenho que informar meu CPF no caixa sempre? Resposta:** Sim. Dessa forma, aumentam as possibilidades de surgirem ofertas exclusivas para o(a) senhor(a). [...]
>
> **7. Existe risco ao digitar o CPF no sistema da Araujo? Resposta:** Não existe risco. A utilização do número de CPF serve especificamente como forma de identificação do cliente para viabilidade de ofertas e comunicação personalizada.
>
> **8. Haverá desconto para medicamentos?Resposta:** Sim. Em breve, os kits de medicamentos também estarão disponíveis no programa Tem + Araujo e serão sinalizados por meio de pop-ups no sistema de balcão. [...]
>
> **12. A Araujo vai ter acesso aos meus dados financeiros? Resposta:** Não. Seu CPF só será usado para habilitar os descontos em nossas lojas." (grifo nosso)

As poucas informações disponíveis no blog da farmácia sobre o programa de descontos "Tem + Araujo" não são suficientes para que o consumidor possa consentir de maneira informada sobre a coleta de seus dados pessoais em troca de descontos.

Dados de consumo que são gerados em farmácias podem revelar aspectos muito significativos da vida de um consumidor, e também podem levar a práticas abusivas incorridas por empresas pertencentes a grandes grupos

econômicos. Informações sobre quando uma pessoa adoece, se possui alguma infecção sexualmente transmissível (IST), doenças crônicas, distúrbios psíquicos, entre diversas outras informações sensíveis, expressadas pelas indicações nas categorias da Classificação Internacional de Doenças (CID)[4] nos receituários, podem, por exemplo, ser inferidas a partir de dados relativos ao hábito de compra de medicamentos. Quando o consumidor fornece seu CPF no caixa, não lhe é informado esse quadro mais amplo sobre como seus dados podem ser utilizados.

Essa situação é ainda mais grave quando se considera que as farmácias sequer possuem termos de uso ou políticas de privacidade para os programas de desconto. Dessa forma, a falta de consentimento qualificado e de transparência sobre a coleta e uso dos dados pessoais do clientes - genericamente, o tratamento dos dados - viola diversas garantias constitucionais e direitos infraconstitucionais relativos à privacidade e proteção do consumidor.

Esta Representação objetiva a atuação do Ministério Público para a tutela dos direitos coletivos e transindividuais relativos à proteção das informações e a vulnerabilidade do consumidor na proteção de seus dados pessoais em relações de consumo. Nesse sentido, vale destacar a precisa observação feita por Alessandro Mantelero, pesquisador do Instituto *Politecnico de Turim*:

> "[...]os usuários não conseguem entender as finalidades e os métodos de processamento de dados. Isso nos leva a reconsiderar o papel da autodeterminação do usuário no processamento de dados, como definido nas décadas de 1980 e 1990. Quando os usuários não são capazes de entender o processamento de dados e seus propósitos, ou não estão em condições de decidir, o seu o papel deve ser reduzido e, inversamente, **o papel das autoridades independentes deve**

[4] O CID é utilizado por médicos, outros profissionais de saúde, pesquisadores e gestores em saúde, empresas, seguros de saúde e organizações de pacientes, para classificar doenças e problemas em saúde nos registros em saúde, de modo uniforme.

> **aumentar**. Na era do Big Data, são as autoridades de proteção de dados, ao invés dos usuários, que detêm o conhecimento tecnológico para avaliar os riscos associados ao processamento de dados e que podem adotar medidas adequadas para reduzi-los. Além disso, **elas estão em melhor posição para equilibrar todos os diferentes interesses** dos vários interessados em projetos extensivos de coleta de dados e de mineração de dados." (grifos nossos)[5]

Com o objetivo de entender quais seriam os reais propósitos da coleta desses dados e como é realizado o seu tratamento, essa prática tem sido investigada em outros municípios do país. O Ministério Público do Distrito Federal, por meio da *Comissão de Proteção dos Dados Pessoais*[6] iniciou investigação contra as dez maiores redes de farmácia do país, sob a suspeita de que os dados pessoais de consumo dos cidadãos estejam sendo repassados a terceiros.[7] Ademais, essa questão também tem sido tema de jornais locais de Belo Horizonte[8]-[9].

2. Dos Direitos Violados

[5] MANTELERO, Alessandro. *The future of consumer data protection in the E.U.Re-thinking the "notice and consent" paradigm in the new era of predictive analytics*. Computer Law & Security Review: nº 30. 2014. pp 643 - 660.
[6] Disponível em: <http://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/comissao-de-protecao-dos-dados-pessoais>
[7] LUIZ, Gabriel. *CPF em troca de desconto: MP investiga venda de dados de clientes por farmácias*. Portal G1. Publicado em 19/03/2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml>
[8] REDAÇÃO. *Solicitação de CPF por farmácias de BH deixa consumidores preocupados e Procon em alerta*. Rádio Itatiaia. Publicado 05/03/2018. Disponível em: <http://www.itatiaia.com.br/noticia/solicitacao-de-cpf-por-farmacias-de-bh-deixa>
[9] MARTINS, Eurico. *Lojas solicitam, mas cliente não é obrigado a digitar CPF* . Jornal O Tempo, Publicado em 05/03/18. <https://www.otempo.com.br/capa/economia/lojas-solicitam-mas-cliente-n%C3%A3o-%C3%A9-obrigado-a-digitar-cpf-1.1580356>

O armazenamento e a utilização de dados pessoais para fins comerciais não configuram um ilícito por si só, pois permitem o surgimento de novos modelos de negócios e serviços ao consumidor. Entretanto, o tratamento de dados pessoais[10] deve estar contido em certos limites de forma a proteger os cidadãos de eventuais abusos, salvaguardando sua privacidade e seus dados pessoais. Tanto o armazenamento quanto o tratamento devem ser informados e consentidos pelo consumidor, ou seja, o titular dos dados.

2.1 Direito à Privacidade e Proteção de dados pessoais

De forma resumida, pode-se entender que a proteção de dados pessoais refere-se a mecanismos (jurídicos, técnicos, entre outros) que objetivam garantir o direito constitucional à privacidade, fornecendo ao cidadão algum nível de controle sobre a utilização de seus dados.

Mesmo que ainda não tenhamos uma Lei Geral de Proteção de Dados Pessoais - apesar de os debates relativos ao PLS 330/2013 e ao PL 4.060/2012 terem ganhado força recentemente no Congresso Nacional[11] - ainda assim, é errôneo afirmar que inexiste no direito brasileiro normas legais e infralegais que garantem a proteção dos dados pessoais dos usuários e consumidores. A ausência de uma lei que regulamente de forma específica a proteção dos dados

[10] O tratamento de dados pessoais pode ser compreendido como "[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" de acordo com o Decreto 8771/16, que regulamenta o Marco Civil da Internet.

[11] Diversas movimentações têm sido realizadas no legislativo brasileiro para a aprovação de uma lei geral de proteção de dados pessoais, demonstrando o interesse latente da sociedade civil em busca de uma lei que busca dar garantias e proteger os dados pessoais.O (1) PL 5.276/2016, o qual teve ampla participação da sociedade civil na formação do projeto, tendo sido apensado ao PL 4.060/2012, recentemente aprovado na Câmara dos Deputados <https://bit.ly/2gbMESN>. Há também o (2) PLS nº 330/2013, atualmente sendo discutido na Comissão de Assuntos Econômicos do Senado <https://bit.ly/2HQNpy8>.

pessoais dos cidadãos, não é suficiente para afastar a tutela jurídica[12]. Diversas são as garantias previstas no ordenamento jurídico brasileiro que dizem respeito à proteção dos dados pessoais:

a) Garantia de acesso e retificação de informações pessoais mantidas em registros de caráter público mediante o remédio constitucional do *habeas data*: artigo 5º, LXXII, da Constituição da República e Lei nº 9.507/1997);

b) Proteção dos dados pessoais dos consumidores: artigos 6º, III e IV; 8º, 12, 43 do Código de Defesa do Consumidor (Lei nº 8.078/1990) e artigo 39, V;

c) Proteção dos dados pessoais de consumidores que realizam compras online de produtos farmacêuticos e proibição do uso de dados pessoais para promoção, publicidade e propaganda: artigo 59 da Resolução da Diretoria Colegiada da Anvisa - RDC nº 44 de 17/08/2009;[13]

d) Tutela do consumidor quanto às suas informações de adimplemento e para a formação de histórico de crédito em bancos de dados por gestores e sistemas de *credit scoring* (Lei nº 12.414/2011);

e) Proteção de dados pessoais dos usuários de internet: artigos 3º, II e III; 7º e 8º do Marco Civil da Internet (Lei n° 12.965/2014);

[12] BIONI, Bruno. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI, São Paulo, 2015. Disponível em: <https://bit.ly/2HP6I5O>

[13] Art. 59. É responsabilidade do estabelecimento farmacêutico detentor do sítio eletrônico, ou da respectiva rede de farmácia ou drogaria, quando for o caso, assegurar a confidencialidade dos dados, a privacidade do usuário e a garantia de que acessos indevidos ou não autorizados a estes dados sejam evitados e que seu sigilo seja garantido.
Parágrafo único. Os dados dos usuários não podem ser utilizados para qualquer forma de promoção, publicidade, propaganda ou outra forma de indução de consumo de medicamentos. Disponível em: <https://www20.anvisa.gov.br/segurancadopaciente/index.php/legislacao/item/rdc-44-2009>

f) Proteção dos dados no âmbito da transparência da Administração Pública: artigo 31 da Lei de Acesso à Informação Pública (Lei n° 12.527/2011);

g) Necessidade de consentimento e exceções (dados indispensáveis para a execução de um contrato ou obrigação legal do fornecedor): artigos 7°, VII e IX, e 16, I, do Marco Civil da Internet;

h) Necessidade de transparência sobre produtos e serviços, bem como sobre a finalidade para a qual os dados são coletados : artigos 7°, VI, VIII e XI do Marco Civil da Internet;

i) Proteção contra a discriminação; e harmonização dos interesses dos participantes nas relações de consumo: artigos 4°, III, e 6°, II, do Código de Defesa do Consumidor;

j) Necessidade de segurança da informação e dos sistemas: artigos 2°, V, e 10, §4°, do Marco Civil da Internet;

Nos últimos 30 anos, diversos países no mundo têm se preocupado com a proteção da privacidade e dos dados pessoais de seus cidadãos, principalmente no contexto atual da sociedade da informação. Nela, são cada vez mais facilitados e menos custosos a coleta, o armazenamento e o tratamento de inúmeras informações sobre os indivíduos. Recentes escândalos de uso não autorizado e indevido de informações pessoais revelam como é necessário que seja garantida uma proteção mínima aos cidadãos.

Um caso paradigmático sobre o tema foi a recente polêmica envolvendo a *Cambridge Analytica*[14], em que foram coletados, sem consentimento, dados de cerca de 87 milhões de estadunidenses por meio de aplicativos no Facebook, para fins de campanha política, publicidade direcionada e manipulação eleitoral

[14]"Entenda o escândalo de uso político de dados que derrubou o valor do Facebook e o colocou na mira de autoridades', BBC Brasil, 20 de Março de 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751> Acesso em 14 de Junho de 2018.

[15]. Casos notórios evidenciam o quanto é necessário o consentimento qualificado e a transparência na coleta de dados, sendo cada vez mais importante que empresas que utilizam esse modelo de negócio sejam transparentes quanto às formas de tratamento que dão a dados pessoais.

Assim, a partir de uma perspectiva de direito comparado, tem sido dado cada vez mais destaque à ideia de consentimento do usuário como pré-requisito para o tratamento de dados pessoais. Desde 1995, por meio da Diretiva 95/46/CE, a União Europeia estabelece certas condições para que o consentimento ao tratamento de dados seja válido juridicamente. Tais condições foram aperfeiçoadas com a entrada em vigor em 25/05/2018 da *General Data Protection Regulation* (GDPR). A regulação europeia estabelece para todos os países membros, no artigo 4º:

> "Art. 4º - Definições - «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;" (grifo nosso)

O conceito de consentimento qualificado tem como finalidade empoderar o titular, de forma a permitir com que ele tenha um mínimo de controle sobre como, para quê, por quem e por quanto tempo seus dados pessoais serão tratados. Parte-se da premissa de que os dados pessoais de um cidadão continuam a integrar a sua personalidade - não podendo ser utilizados de qualquer forma, como se fossem uma mera *commodity* no mercado.

De forma semelhante, o art. 7º do Marco Civil da Internet, também apresenta requisitos ao ato de consentimento:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> [...]

[15] Sobre essa questão, verificar o blog do IRIS: www.irisbh.com.br

> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> [...]
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;" (grifo nosso)

Essas noções de consentimento expresso, alicerçadas no preceito da "autodeterminação informativa", estabelecem que, quando alguém consente ao tratamento dos seus dados pessoais por uma determinada razão, a empresa que os coleta só poderá efetuar o tratamento dos mesmos conforme as finalidades para as quais a coleta dos dados pessoais foi consentida. Além disso, deve ser possível que o indivíduo revogue o consentimento sobre o uso de seus dados a qualquer momento, a semelhança do art. 7º, X da Lei 12.965/2014.

Nos EUA, de forma resumida, não há uma lei geral sobre proteção de dados pessoais. Na verdade, há leis setoriais, tanto no âmbito federal como estadual, que tratam de temas específicos como dados financeiros, saúde, criança e adolescente, entre outros. Ademais, há também a prática de autorregulação dos diversos setores econômicos na área de privacidade e proteção de dados pessoais, a qual exerce poder de *soft law*. Na área de saúde, a principal legislação é a lei federal *Health Insurance Portability and Accountability Act* of 1996 (HIPAA), a qual define os padrões de proteção mínimos aplicáveis no país, que podem ou não ser aprofundados por leis estaduais.

No geral, a HIPPA define o que são dados pessoais de saúde; as situações em que esses dados podem ser utilizados ou compartilhados; os direitos de privacidade e quando deve ser obtido o consentimento dos cidadãos para uso dos dados; os padrões mínimos de segurança da informação para as operações de armazenamento e transmissão dos dados de saúde; o direito de acesso da

pessoa aos seus dados de saúde armazenados por uma instituição, e se e com quem eles foram compartilhados; entre outros.[16]

Em um breve trecho, cita-se como exemplo a política de privacidade da drogaria estadunidense *Hartig Drug Store*, em conformidade com a HIPAA. Como um dos indicativos da importância do tema pode-se destacar o fato de que a própria drogaria possui um setor específico para lidar com o tema de proteção de dados do cliente (*privacy officer*):

> **"Nossas Responsabilidades**
> - Somos obrigados por lei a manter a privacidade e a segurança de suas informações de saúde protegidas.
> - Avisaremos você imediatamente caso ocorra uma violação de segurança de nosso dados que possa ter comprometido a privacidade ou a segurança de suas informações.
> - Devemos seguir os deveres e práticas de privacidade descritos neste aviso e fornecer uma cópia do mesmo.
> - Nós não usaremos ou compartilharemos suas informações para além das práticas descritas aqui, a menos que você nos dê seu consentimento. Se você nos der seu consentimento, ainda sim você pode mudar de idéia e retirá-lo a qualquer momento. Deixe-nos saber por escrito, se você mudar de idéia."[17]

2.2 Direito à Informação e Finalidade do Uso dos Dados Pessoais

Um dos principais riscos ao consumidor refere-se ao tratamento e cruzamento ilimitado de um dado fornecido somente em contexto e finalidade específico. No caso desta Representação, se o consumidor fornece seu CPF com

---

[16] "Muitas leis regulam a privacidade de informações médicas nos EUA. Embora essas leis ofereçam alguma proteção, no geral, elas operam mais para garantir o fluxo de informações em todo o setor de saúde do que garantir a privacidade dos indivíduos.
Além disso, essas leis geralmente se aplicam apenas a informações médicas pessoais nas mãos de tipos específicos de instituições, como médicos ou hospitais. Assim, por exemplo, as informações que você fornece a uma rede social ou a um site de busca, em uma sala de bate-papo ou em uma discussão em um site sobre uma doença, geralmente não são protegidas pelas leis de privacidade médica existentes nos EUA." (tradução e grifo nossos). ELECTRONIC FRONTIER FOUNDATION (EFF). *The Law and Medical Privacy.* Acessado em: 16/06/2018. Disponível em: <https://bit.ly/2lkD8MG>.

[17] HARTIG DRUG STORE. *Privacy Policy.* Acessado em: 15/06/2018. Disponível em: <https://bit.ly/2MGsahc>

a finalidade de receber um desconto, ele deveria ser informado sobre (i) **como** seus dados pessoais de consumo serão tratados, (ii) **para qual finalidade**, e (iii) **por qual período de tempo**. Apesar de a drogaria Araujo informar em seu blog que "*o CPF é transformado em um código interno e nenhum funcionário Araujo ou terceiro tem acesso*", em nenhum momento essa informação é repassada ao cliente pelos atendentes no momento da compra. Além disso, não é possível verificar a efetividade dessa informação, visto que os consumidores não possuem acesso e mecanismos suficientes para averiguar a aplicação de tal medida. Assim, a mera requisição do CPF, sem nenhuma informação sobre as condições do tratamento dos dados e sua finalidade, viola o direito à informação do consumidor, artigo 6º, III, do Código de Defesa do Consumidor:

> Art. 6º São direitos básicos do consumidor:
> [...]
> III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem

Novamente, deve ser feita uma analogia com o Marco Civil da Internet, quanto à importância do acesso à informação sobre o tratamento de dados dos cidadãos, principalmente porque o projeto de lei foi inspirado, em parte, na legislação da União Europeia, Diretiva de Proteção de Dados Pessoais 95/46/CE , que possui padrões elevados de proteção:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> [...]
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;" (grifo nosso)

Deve-se investigar como estes dados estão sendo tratados pelas farmácias, bem como se realmente eles não são repassados a terceiros, como, por exemplo, para empresas de avaliação de crédito, fornecimento de planos de saúde e também às denominadas *data brokers*[18]. Estas últimas são empresas que sobrevivem única e exclusivamente da coleta e revenda de dados pessoais para os mais diversos fins, evidenciando o quão robusto é o mercado para dados pessoais, além de quanto incentivo há para que empresas comercializem dados sem o consentimento expresso de seus titulares.

A finalidade de recolhimento do dado, quais as limitações aplicadas ao tratamento, e eventuais repasses destes a terceiros são informações que devem ser expostas de maneira transparente ao consumidor, para que ele possa sopesar eventuais custos e benefícios. Assim, se a opção for pela manutenção do programa de descontos, deve-se treinar funcionários para que repassem as condições dos programas de benefícios por meio de CPF e criar mecanismos de transparência para demonstrar a real finalidade e uso desses dados, permitindo ao consumidor que faça uma escolha minimamente informada e consentida com os reais intuitos da coleta.

2.3 Debate legislativo sobre a proteção de dados no Brasil

Nos últimos meses, a privacidade e a proteção de dados pessoais têm sido assunto de diversas sessões na Câmara dos Deputados e no Senado Federal, o que evidencia tanto a importância dessa temática quanto à urgência e

[18] Vermont foi o primeiro estado nos EUA a aprovar, ainda em 2018, uma lei específica para regular a atuação de *data brokers.* A lei define o que são *data brokers,* a obrigatoriedade das empresas se registrarem perante as autoridades estaduais, o dever de transparência para com os consumidores sobre o tratamento de seus dados, quando é possível se retirar do tratamento, e o dever de informar os afetados em caso de vazamento de dados. COLDEWEY, Devin. *Vermont passes first law to crack down on data brokers.* Techcrunch. 27/05/2018. Acessado em: 04/06/2018. Disponível em: <https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/>

necessidade de consolidação de uma lei geral para a proteção desses direitos no Brasil. Na Câmara dos Deputados, recentemente foi aprovado o PL 4.060/12, subsequentemente apensado ao texto do PL 5.276/16[19] - que agora segue para o Senado Federal. O Senado também discute o PLS 330/13, e ambos os projetos de lei, relacionados à proteção de dados pessoais, seguem em tramitação.

Esses projetos estabelecem garantias e deveres para a coleta de dados pessoais em território nacional, consolidando garantias que esparsamente já existem no ordenamento e, dessa forma, fixando normas mais rígidas quanto ao consentimento, a finalidade e o tratamento dos dados pessoais. O PL 5276/16, em seu artigo 5º, VII, define consentimento como: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Além disso, o PL estabelece exigências adicionais com relação aos dados sensíveis[20], determinando que para o tratamento desses dados é necessário haver "consentimento livre, inequívoco, informado, **expresso e específico pelo titular"** (Art. 11). A definição de dados sensíveis no PL guarda forte sintonia com a Convenção do Conselho da Europa nº 108, denominada "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais", que define dados sensíveis no artigo 6º como:

> Dados pessoais que revelem a origem racial, opiniões políticas, religiosa ou de outras crenças, bem como dados relativos **à saúde pessoal ou à vida sexual** não podem ser processados automaticamente ao menos que leis nacionais estabeleçam garantias adequadas. O mesmo se aplica a dados pessoais relativos a condenações criminais.

[19] Ver mais em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. E para a versão final do texto do PL: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1665276&filename=Tramitacao-PL+4060/2012>

[20] Idem.

Essa diferenciação entre dados sensíveis é extremamente importante para esta Representação, evidenciando que em diversas abordagens legislativas os dados relacionados à saúde do consumidor possuem uma proteção e tutela especial, evidenciando a importância na responsabilidade e transparência no uso e armazenamento desses dados.

A ausência de consentimento para uso desses dados é, por si só, um fator extremamente preocupante. Ela tem sido prática conduzida por diversas dessas empresas atuantes no segmento das drogarias. Alia-se, ainda, à falta de determinação do tempo pelo qual os dados serão armazenados e da possibilidade ou não de remoção desses dados. Isso cria um cenário de incertezas e de falta de informações em relação ao real intuito do programa de descontos, comercialmente oferecido pela empresa. Para além da falta de consentimento, observam-se a obscuridade e a completa falta de informação sobre como esses dados são tratados e utilizados e também sobre quais são seus reais propósitos e aplicações, o que possibilita que sejam utilizados para diversas finalidades desconhecidas por parte dos titulares - clientes/consumidores.

Exemplificadamente, seria possível visualizar o seguinte cenário: um cruzamento entre o CPF de um cliente e seu perfil de compras de remédios poderia mostrar para uma prestadora de plano de saúde que ele tem uma condição médica específica, como a discriminação positiva do consumidor/paciente em virtude do enquadramento de sua enfermidade na CID. Igualmente, a interpretação desses dados poderia reforçar perfilamentos[21] discriminatórios, em um sistema financeiro, e revelar que o titular dos dados

[21] Pode ser compreendido como qualquer forma de tratamento automatizado de dados de caráter pessoal que consista na utilização destes dados para avaliar determinados aspectos pessoais relativos a uma pessoa, especialmente para analisar ou prever elementos referentes ao desempenho profissional, à situação econômica, à saúde, às preferências pessoais, aos interesses, à confiabilidade, ao comportamento, à localização ou aos deslocamentos. Um exemplo de empresa que utiliza do perfilamento é o caso do Serasa Experian, que pode ser acessado em: https://encripta.org/folheto-serasa.pdf

sofre de uma doença terminal. Desse modo, seria possibilitar a cobrança de juros mais elevados em contratos de empréstimo, em razão da informação sobre os riscos de saúde daquele cliente.[22]

3. Conclusões

Fica evidente que o consentimento de um cliente com determinado modelo de tratamento de dados pessoais, deve ser precedido e acompanhado de uma série de requisitos, de forma a se garantir o direito à privacidade do consumidor. O conceito de consentimento informado não é novo no debate internacional sobre proteção de dados pessoais[23]; contudo, é um dos pilares fundamentais na proteção dos usuários e é recepcionado pelo ordenamento jurídico brasileiro.

Para melhor endereçar o objeto desta Representação, é preciso considerar as críticas ao posicionamento que delega unicamente à pessoa natural (consumidor) a responsabilidade pela proteção dos seus dados. Conforme explica a pesquisadora Eoin Carolan, da *University College* em Dublin, sobre as limitações do consentimento:

> "[...] o usuário individual enfrenta várias barreiras para a formação e articulação de preferências online racionais e autônomas. De fato, a literatura psicológica sugere que o usuário individual é significativamente suscetível a formas de manipulação online. Nesse cenário, **uma abordagem da privacidade ou da proteção de dados pessoais que coloque ênfase substancial no consentimento não é neutra. Pelo contrário, é provável que funcione como uma estrutura**

[22] Ver mais em: https://gizmodo.uol.com.br/ministerio-publico-cpf-farmacia/

[23] O conceito de consentimento sofreu transformações ao longo dos anos no direito europeu, conforme os problemas de proteção de dados pessoais foram se complexificando. Resumidamente, este conceito passou por três definições desde de 1995 na UE: (1) consentimento presumido, (2) consentimento informado, e (3) consentimento ativo. Para uma análise resumida ver: PORTO, Odélio Jr. *Tipos de Consentimento e Proteção de Dados Pessoais: Um Breve Histórico.* Instituto de Referência em Internet & Sociedade (IRIS). 11 de junho de 2018. Disponível em: <http://irisbh.com.br/tipos-de-consentimento-e-protecao-de-dados-pessoais/>

> **permissiva para práticas intrusivas à privacidade online**." (grifos nossos)[24]

Apesar de crível a ideia de que a autodeterminação do consumidor é um fator que não pode ser desprezado, ainda assim há casos em que as autoridades públicas devem intervir, o que se espera com a presente representação. Esse papel é notadamente observado na União Europeia, em que cada Estado Membro possui uma Autoridade de Proteção de Dados Pessoais incumbida das funções de proteção de dados pessoais[25]. Na situação descrita por esta Representação, é dever constitucional do Ministério Público efetivar, na tutela dos interesses coletivos e transindividuais, o direito à informação do consumidor, de forma que ele esteja suficientemente informado sobre como seus dados pessoais serão tratados, e quais as possíveis consequências desse tratamento, como usos e processamentos por terceiros.

4. Recomendações

Em vista do exposto anteriormente, e da necessidade de observância das garantias e proteções constitucionais e legais do consumidor - artigos 5º, X e XXXII, da Constituição Federal, e artigos 6º, III e IV, 8º, 12, e 43 do Código de Defesa do Consumidor - recomendam-se as seguintes ações por parte do Ministério Público de Minas Gerais:

1. Que proceda à abertura regular de um inquérito civil, ou, a seu juízo, ao ajuizamento de uma ação civil pública endereçando, dentre outros, a

[24] CAROLAN, Eoin.*The continuing problems with online consent under the EU's emerging data protection principles* .Computer Law & Security Review 32 (2016). pp 462 - 473. Acessado em: 07/06/2018. Disponível em: <https://bit.ly/2JpqFle>

[25] Artigo 51º da Regulação Geral de Proteção de Dados (GDPR): "Autoridade de controlo - 1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União («autoridade de controlo»). Acessado em: 07/06/2018. Disponível em: <https://bit.ly/2LsogHg>.

obrigação de fazer às empresas do segmento de drogarias atuantes no estado de Minas Gerais de esclarecer aos clientes, no momento da compra (por meio de folhetos, explicação oral etc.), as condições de participação dos programas de descontos, além de indicar em seus respectivos websites a precisa localização dos termos de uso;

2. Que se certifique que os termos de uso sejam disponibilizados de forma adequada, inteligível e de fácil acesso aos consumidores e expliquem: i) para que finalidade e como os dados pessoais serão utilizados; ii) se eles são ou não repassados a terceiros; e iii) que o estabelecimento se responsabiliza pela segurança das informações coletadas e armazenadas. Atualmente as farmácias disponibilizam apenas, em blogs, seções de "perguntas e respostas" - os conhecidos "FAQs";
3. Que sejam elaboradas pelas farmácias políticas de transparência sobre o armazenamento, a coleta e o uso desses dados pessoais, demonstrando aos cidadãos os reais intuitos e objetivos dessa coleta em cada um dos programas de fidelidade disponibilizados;
4. Que eventuais acidentes na segurança das informações, que possam afetar os clientes, sejam a eles informados, e, nos casos em que houver direitos afetados, que o MP-MG ou eventual Autoridade de Proteção de Dados seja comunicado e/ou notificado pelas empresas;[26]
5. Que as redes de farmácias prestem esclarecimentos ao Ministério Público, se os dados são ou não repassados, ou ainda comercializados, a terceiros sem o prévio e devido consentimento dos consumidores, de forma análoga ao que estabelece o artigo 7º, inciso VII, da Lei nº 12.965/2014 (Marco Civil da Internet);

[26] Verificar a prática do MP-DF sobre a necessidade de notificação sobre incidentes de segurança de dados (data breach notification) e o caso de vazamento de dados dos clientes da Netshoes, no qual foi imposta obrigação de informar os consumidores afetados pelo incidente. Disponível em: <https://bit.ly/2sL3gnn>

6. Que as redes de farmácias prestem esclarecimentos ao Ministério Público sobre, e especificamente, como os dados são coletados, tratados e armazenados, e quais as medidas de segurança adotadas em relação aos dados.

Termos em que,
Respeitosamente,
Subscrevemos.

Fabrício B. Pasquot Polido
Conselheiro Científico do Instituto de Referência em Internet & Sociedade

Luiza Couto Chaves Brandão
Diretora do Instituto de Referência em Internet & Sociedade

Odelio Porto Júnior
Vice-diretor do Instituto de Referência em Internet e Sociedade

Davi Teófilo Nunes de Oliveira
Pesquisador do Instituto de Referência em Internet e Sociedade

Anexo I

Versão adaptada e atualizada das perguntas feitas à certas redes farmacêuticas pela Comissão de Proteção dos Dados Pessoais do MPDFT.

1) A Rede [XXXXXX] é adepta da prática de concessão de descontos nas compras de produtos para os clientes previamente cadastrados em suas bases de dados? Os descontos são concedidos em um mesmo percentual para clientes não cadastrados ou que não desejam se cadastrar?

2) Qual o objetivo primordial da citada prática indicada no item 1: descontos em troca de dados?

3) A empresa armazena informações sobre todas as compras de seus clientes cadastrados (histórico de compras), online e no balcão?

4) Algum software específico é utilizado para coletar, armazenar e tratar estes dados pessoais sensíveis?

5) De que forma os bancos de dados dos clientes são armazenados? Indicar as medidas de segurança utilizadas atualmente para a proteção dos dados pessoais, inclusive procedimentos de criptografia.

6) Os dados pessoais dos clientes (nome, telefone, CPF, endereço, histórico de compras, etc) são compartilhados com outros estabelecimentos farmacêuticos, seja do mesmo grupo econômico da empresa ou de grupos econômicos diversos?

7) Como funcionam os programas de benefícios ou descontos oferecidos pela empresa, em troca de dados pessoais? Explicar de forma detalhada, para além do que é apresentado nos “FAQs” da empresa;

8) Os dados pessoais dos clientes são compartilhados com empresas externas, não ligadas ao setor farmacêutico? Em caso positivo, por quais motivos?

9) Os dados pessoais dos clientes são de alguma forma comercializados? Se sim, quem são os adquirentes desses dados e quais as modalidades de transações e negócios embasando a comercialização.

10) Os dados pessoais dos clientes são compartilhados com o Governo (Federal, Estadual, Municipal)? Em caso positivo, por quais motivos ou obrigações legais?