O DIREITO À PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DE VIGILÂNCIA: A NECESSIDADE DE UM MARCO REGULATÓRIO COMO DEVER PRESTACIONAL DO ESTADO DEMOCRÁTICO DE DIREITO

Ricardo Ruiz Schreinert, Regina Linden Ruaro[1] (orientador)

[1]*Faculdade de Direito, PUCRS, bolsa Probic/Fapergs.*

Resumo

O importante divisor de águas acerca do tratamento necessário à proteção ao direito à privacidade é a Era da Informação. Antes dela, adotava-se a tradicional divisão binária entre público e privado a qual associava o direito à privacidade (direito imaterial) ao direito à propriedade privada (direito material). Segundo essa distinção, o cidadão apenas estaria protegido pelo direito à privacidade quando estivesse em sua propriedade privada. Caso estivesse em um local público, sairia da sua esfera de privacidade, portanto estaria na esfera pública consentindo na exposição de sua privacidade. Após a Era da informação, com o desenvolvimento de tecnologias de informação, essa antiga divisão binária entre privado e público tornou-se obsoleta, uma vez que não mais se obtém sucesso em proteger um indivíduo em sua propriedade privada, já que, por exemplo, um terceiro pode estar captando suas imagens através de uma filmadora ou suas informações podem estar sendo repassadas virtualmente. O que não pode mais ocorrer é a aplicação da tradicional divisão binária entre o público e o privado, pois apesar desta ser uma regra clara e que permite uma fácil resolução do tema, a simplicidade dessa visão não se compatibiliza com a Era da Tecnologia.

Frente a essas transformações decorrentes do desenvolvimento informático e tecnológico, faz-se necessário uma nova interpretação acerca dos meios necessários à proteção da privacidade e da intimidade, ou seja, a privacidade é um direito inerente ao indivíduo, não importando onde este esteja. Nesse sentido, os direitos da personalidade da intimidade e privacidade não podem mais ser confundidos com a esfera de propriedade privada, já que, como já dito, são direitos da personalidade e, portanto são inerentes de qualquer cidadão.

Conforme exposto acima, fica evidente a necessidade de instrumentos que possam, satisfatoriamente, proteger o direito à privacidade. Em decorrência do desenvolvimento tecnológico e da criação de redes de informação, o direito à privacidade poderá estar sendo posto em risco, principalmente e especificamente, através de uma atividade: a formação de bancos pessoais de dados que possibilitam a criação de perfis dos seus titulares. Portando, a esfera de proteção do direito à privacidade, frente à Era da Tecnologia e à Sociedade de Vigilância, reproduzir-se-á no direito à proteção pessoal de dados, tema que será abordado.

Recentemente, foram sendo aprovadas normas que envolvem aspectos particulares da reserva da intimidade da vida privada, especificamente respeitantes à proteção de dados ou informações pessoais. Não se trata, todavia, da larga esfera de proteção do direito à privacidade ou à intimidade, protege-se, neste caso, um direito proveniente dessas esferas, a autodeterminação informativa (Recht auf informationelle Selbstimmung). Em muitos contextos, este direito aparece referido ao tratamento de informações mediante o uso da informática. Para assegurar o direito à intimidade e à privacidade das pessoas no tratamento pessoal de dados, tantos as normas nacionais como internacionais acordam em desenvolver um direito fundamental autônomo denominado de autonomia da vontade ou de autodeterminação informativa1, que se define como um direito fundamental frente a potenciais ataques à dignidade e à liberdade da pessoa de uma utilização ilegítima de dados pessoais, que visa garantir a pessoa o poder de controle sobre seus dados pessoais e sobre a sua utilização e destino, com o objetivo de prevenir ilícitos e prejudiciais à dignidade e direitos "2. O direito à autodeterminação informativa é composto de dois elementos3: um de caráter negativo, os princípios que regulam a qualidade de tratamento dos dados, e outro elemento de caráter positivo, ou seja, o direito dos interessados que podem ser assegurados através instrumentos como o habeas data. Abaixo, estão alguns dos princípios que garantem um devido tratamento dos dados genéticos, os quais são fundamentais para se salvaguardar direitos fundamentais.

[1] La Carta de los Derechos Fundamentales de la Unión Europea ha consagrado en su artículo 8º como un derecho fundamental autónomo e independiente, tanto del derecho a la intimidad como del derecho al secreto de las comunicaciones, el derecho a la protección de los datos personales o, lo que es lo mismo, el derecho a la autodeterminación informativa. En el ámbito español es clara la postura del Tribunal Constitucional en orden a considerar el derecho a la autodeterminación informativa o libertad informática como un derecho fundamental autónomo distinto del derecho a la intimidad.

[2] Sentencia del Tribunal Constitucional Español 192/2000, de 30 de noviembre.

[3] Vid. GARRIGA DOMÍNGUEZ, A.: *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004.

No início dos anos 70, a Resolução n.º 428 da Assembléia Parlamentar do Conselho da Europa já se mencionava a necessidade de proteger a vida privada face às possibilidades criadas pelo uso de meios informáticos.

Ademais, a fim de garantir o direito à autodeterminação informativa, necessário à tutela de informações pessoais compiladas em bancos de dados, a União Européia estabeleceu três Diretivas comunitárias, a Diretiva 95/46/CE, a Diretiva 97/66/CE e Diretiva 2002/53/CE, que determinam metas a serem alcançadas a uma necessária regulação da proteção pessoal de dados. Ademais, a União Européia estabelece vários princípios que norteiam a regulamentação do tratamento à proteção pessoal de dados, o principal deles é o princípio da finalidade e relevância.

É necessário respeito escrupuloso aos princípios de relevância e finalidade, de modo que os dados pessoais só podem ser recolhidos e tratados em conformidade com um fim legítimo, explícito e específico. Além de coletados e processados, os dados estão relacionados à finalidade prosseguida e, portanto, deve ser "adequada e não devem exceder os fins para os quais foram coletados"4. Assim, os dados devem "servir" à finalidade para a qual eles são obtidos, de forma que existe uma "ligação clara entre a informação que é recolhida e (...) a finalidade para a qual a aplicação"5. Ou seja, a informação só pode ser coletada e tratada, quando os dados são adequados em relação ao alcance e finalidade para aos quais eles foram obtidos, bem como deve haver garantia de que não serão utilizados para fins incompatíveis com aqueles para os quais foram coletados.

Pode-se dizer que idéia de autodeterminação informativa consolidou-se na Alemanha, em 1983, em meio a um censo geral de 160 perguntas que objetivava acarear os dados pessoais da população com seu registro civil. Entretanto, uma sentença da Corte Constitucional suspendeu-o e, posteriormente, considerou-o inconstitucional, sob o argumento de que os dados pessoais recolhidos foram utilizados ao mesmo tempo para fins estatísticos e administrativos, circunstância que caracterizava desvio de finalidade, impedindo que o cidadão pudesse conhecer o efetivo uso de suas informações. Através desse acontecimento, surge a autodeterminação informativa como sendo o direito dos indivíduos de decidirem, por si próprios, quando e dentro de quais limites seus dados pessoais poderão ser utilizados.

---

[4] PÉREZ LUÑO, A.E.: *Los derechos humanos en la sociedad tecnológica,* en LOSANO, M. y otros: *Libertad informática y leyes de protección de datos,* Centro de Estudios Constitucionales, Madrid, 1990, *p. 166.*

[5] LUCAS MURILLO DE LA CUEVA, P..: *Informática y protección de datos personales,* Cuadernos y Debates nº 43, Tecnos, Madrid, 1993, p. 65.

A proteção pessoal de dados no ordenamento jurídico brasileiro, ao contrário do modelo de proteção da União Européia, é uma estrutura complexa e não unitária, apresentando diversos institutos esparsos e setoriais, os quais são derivados dos princípios constitucionais e direitos fundamentais do texto constitucional brasileiro. No tocante à proteção pessoal de dados, talvez seu principal instrumento de regulação seja o habeas data, remédio constitucional brasileiro previsto em seu art. 5º, inc. LXXII. Através desse recurso, o titular dos dados ou seu representante podem conhecer e, se necessário, retificar as informações compiladas no banco de dados.

É necessário ressaltar, entretanto, que o habeas data possui algumas limitações e paradigmas, (alguns superados, outros não) seja por sua confusa redação no texto constitucional, seja por ser considerado por alguns autores como remédio simbólico.

Para Luiz Roberto Barroso6, tratava-se de um remédio de valor simbólico, já que seus efeitos já eram percebidos em recurso já existente, o mandado de segurança. José Carlos Barbosa Moreira corrobora tal consideração ao alegar que, no período de nove anos em que o habeas data não possuía regulamentação, foram utilizadas as normas do mandado de segurança.

Ademais, a ação do habeas data permanece estagnada na esfera do binômio acesso-retificação, não acompanhando o desenvolvimento do sistema da sociedade de vigilância e faltando-lhe especificações mais precisas sobre seu parâmetro de atuação.

Além do habeas data, há também outro instrumento utilizado na proteção pessoal de dados no Brasil, embora regulamente apenas o setor mercantilista frente à proteção pessoal de dados. O Código de Defesa do Consumidor, em seus artigos 43 e 44, regulam a manutenção dos bancos de dados e cadastros de consumidores, estabelecendo garantias.

Os outros direitos do consumidor estabelecidos pelo CDC no que toca à proteção de seus dados pessoais são os direitos de acesso (BENJAMIN et al., 2007, p. 413) e de retificação (BENJAMIN et al., 2007, p 416), que possibilitam a ele consultar toda e qualquer informação pessoal a seu respeito armazenada "em cadastros, fichas, registros e dados pessoais e de consumo arquivados" e, no caso de encontrar alguma incorreção, solicitar a retificação do dado (Artigo 43, caput e §3º). Na hipótese de lhe ser negado o exercício de tais direitos, o consumidor poderá se valer dos procedimentos judiciais ordinários (Artigo 43, § 4º) ou da já citada ação de habeas data. Entretanto tais garantias dispostas pelo ordenamento

[6] Danilo Doneda. Iguais mas separados: o habeas data no ordenamento brasileiro e a proteção de dados pessoais. Pag. 21.

jurídico brasileiro não são suficientes a uma proteção pessoal de dados desejável, além disso no caso do CDC, sua proteção é setorial abrangendo apenas dados de consumidores. Ainda estão totalmente desprotegidos os dados pessoais nas outras relações civis ordinárias em relação ao poder de ingerência do estado.

O desenvolvimento tecnológico, principalmente na área da informática, proporcionou condições de analisar o perfil das pessoas através de dados pessoais, uma atividade bastante útil ao Estado, que poderia melhor planejar suas políticas públicas com o conhecimento dessas informações, contudo a privacidade do cidadão estaria sendo posta em risco, já que se estaria formando um estado super informado. Dessa maneira, há de se equilibrar dois interesses, o público (do Estado) que passaria a dispor de um instrumento para melhor aplicar suas políticas públicas, e o privado que protege os direitos individuais do cidadão. De outra banda, vale ressaltar que a Sociedade de Vigilância não se fundamenta apenas no Estado como ente observador e seus cidadãos como sujeitos observados, mas também entre particulares, sendo um deles o observador e o outro o observado. A tecnologia desenvolveu-se, em alta escala, de sorte que podemos encontrar vários computadores espalhados pelas escrivaninhas de várias famílias. Agrega-se isso ao fato de que as pessoas da Sociedade de Informação se adaptam, cada vez mais cedo, à utilização desses instrumentos, muitas vezes, participando de redes sociais, o que implica alto fluxo de informações sendo compartilhado com o restante da sociedade.

Ressalta-se, entretanto, que, mesmo que existam instrumentos que possibilitem razoável regulamentação no que tange à proteção de bancos de informação alheia, a privacidade das pessoas fica desprotegida diante da sua vontade em dispor de elementos de sua intimidade, entre outras palavras, a proteção da privacidade, atualmente baseada na autodeterminação informativa e na confiabilidade de dados, esvanece diante da boa vontade dos indivíduos em fornecer seus próprios dados pessoais.

Importante ressaltar possíveis motivos pelos quais as pessoas dispõem de seus direitos individuais. Primeiramente, há de se considerar as constantes ameaças de terrorismo que geraram insegurança generalizada no hemisfério norte. Com isso, sentindo-se ameaçados e com a promessa do Estado de uma maior fiscalização dos meios de comunicação a fim de evitar que novos ataques ocorram, as pessoas permitiram que fossem realizadas ingerências do Estado nos seus dados pessoais, respeitados os princípios, em síntese, (RODOTÀ, 1999. p. 62; SAMPAIO, 1997, p. 509) da publicidade, da exatidão, da finalidade, do livre acesso e princípio da segurança física e lógica. No caso dos países do hemisfério Sul, o tratamento de

dados pode ser instrumento de auxílio à administração pública no combate ao gradativo aumento da criminalidade e da violência.

Em segundo plano, há o desejo de inserção no mundo tecnológico e, conseqüência deste, o medo de exclusão social, através da exclusão digital.

Por ultimo e mais importante, há a influência demasiada da mídia, tanto por parte dos meios de telecomunicação quanto pelos informáticos, já que essa passa a sensação de que ser observado acarreta a idéia de relevância social. Segundo David Lyon, o método panóptico (observação de uma maioria por uma minoria) é legitimado pelo sinóptico (observação de uma minoria por uma maioria) e vice-versa. Analisando o fato por esse viés, percebe-se que a mídia, principalmente através da televisão, desencadeia nas pessoas a escopofilia, ou seja, a arte amar quem está sendo observado e, ao mesmo tempo, o desejo de ser observado, aliado ao "voyeurismo7. Portanto, verifica-se que a cultura das sociedades ocidentais, ao serem influenciadas pela mídia, relativiza as ingerências cometidas na esfera da privacidade das pessoas, em prol da liberdade de expressão e do desejo de ser observado, de maneira que, se um indivíduo consente que sua vida privada ou seu corpo sejam colocados à mostra, já que isso é bem visto por uma sociedade em geral, também permitirá que seus dados pessoais sejam violados.

Ademais, através da ingerência nas informações alheias, dependendo do conteúdo dos dados, podem ser violados outros direitos fundamentais além da privacidade ou da intimidade. Existem determinados dados que denotam maior vulnerabilidade e potencialidade discriminatória, por revelarem aspectos de raça, etnia, religião, ideologia política, etc., sãos os chamados dados sensíveis. Nesse sentido, direitos fundamentais como a igualdade e liberdade também podem ser expostos em risco.

Tal consideração também é convincente para explicar a indiferença das pessoas em relação tanto à ingerência do Estado e como do mercado capitalista no tratamento de seus dados pessoais.

Nesse contexto, percebe-se que há vetores de pressão acerca da utilização dos bancos de dados pessoais, entre eles, o Estado e as empresas privadas. O Estado, como já dito, com o propósito de melhorar o planejamento de suas políticas públicas e de sanar problemas sociais como combater a criminalidade e proporcionar condições razoáveis de saúde pública (sem

[7] Vigilância e Visibilidade: Espaço, Tecnologia e Identificação. In. 11 de setembro sinóptico e escopofilia: observando e sendo observado. Pag. 133.

contar as situações de interesse público); as empresas privadas vêem os bancos dados pessoais como uma oportunidade de elevar seu potencial de vendas através da classificação de perfis de seus consumidores e, dessa maneira, calcular seu potencial de consumo.

Dessa maneira, considerando que a atual proteção pessoal de dados está baseada na autonomia informativa e na confiabilidade de dados, a ausência de disciplina legislativa acerca da matéria, influenciada por intervenções estatais em prol do interesse público, transfere ao mercado a tarefa de auto regulamentá-la[8]. Nesse sentido, verifica-se que as razões do Estado compatibilizam-se com a lógica de mercado.

Tendo em vista o exposto, verifica-se que a legislação brasileira vigente é insuficiente à devida proteção e regulação dos dados pessoais, portanto, a fim de encontrarmos diretrizes à proteção da livre circulação de dados pessoais, analisaremos o modelo Europeu de proteção de dados pessoais, mais especificamente o português. Para tanto, é necessário demonstrar a evolução doutrinária do direito à autodeterminação informativa, bem como da mudança de paradigma por parte dos órgãos julgadores e legisladores em relação à livre circulação de dados pessoais.

[8] Revista da Faculdade de Direito – UFPR, Curitiba, n. 47, p. 148, 2008. In Proteção Jurídica de Dados Pessoais: a Intimidade sitiada entre o Estado e o Mercado, José Antônio Peres Gediel e Adriana Espíndola Corrêa.