



Responsabilidade derivada de seu controle

Durante o transcurso de nossas vidas, todos nós, seres humanos, somos obrigados a deixar registros de nossas atividades. Os fatos sociais dos quais participamos, muitas vezes só indiretamente, vão ficando registrados e as informações sendo armazenadas de diversas formas.

Com o nascimento, o indivíduo fornece o primeiro registro de sua passagem pela terra, mas outros vão se sucedendo até a sua morte e, mesmo, até depois dela. Ao nascer, a pessoa é identificada por um nome, seu primeiro atributo informacional (digamos assim), que logo vai se somando a outros, como idade, estado civil, profissão, ocupação, rendimentos, propriedades, entre tantos outros. Se o fato do nascimento é registrado em cartório, inúmeros outros dados que guardam relação ou atestam algum aspecto da vida da pessoa vão sendo colecionados e armazenados enquanto ela vive. Se é para entrar em um colégio, seus dados pessoais precisam ser fornecidos e ficam armazenados nos registros da entidade educacional; se pretende obter um emprego, também tem que fornecer seus dados pessoais ao empregador; o mesmo acontece quando intenta filiar-se a uma associação recreativa, a um sindicato, partido político, seita religiosa ou qualquer outra agremiação. Os seus dados pessoais vão sendo paulatinamente coletados e arquivados em bancos de dados que são utilizados e manipulados por outros indivíduos.

A compilação e o processamento de dados sempre despertou certa preocupação pela razão de que podem afetar o direito à intimidade das pessoas. Por essa razão, o controle dos bancos e sistemas de arquivo de dados pessoais desde cedo constituiu objeto do Direito, no sentido de definir a responsabilidade dos controladores desses sistemas quanto ao uso da informação coletada. Mas é a partir do momento da revolução informática que essa matéria passa verdadeiramente a representar tema de proa para o mundo jurídico. Os antigos fichários manuais são substituídos por bases e arquivos de dados computadorizados, com vantagens imensas no que tange ao acesso e à possibilidade de cruzamento dos dados. Um dado isolado, sem relação com qualquer outro que permita a construção de ilações, não tem o mesmo valor da informação trabalhada e que seja resultado da combinação de variados informes. Os bancos de dados informatizados permitem que os registros neles contidos possam ser classificados segundo diferentes critérios e, desse modo, combinados entre si, num cruzamento que resulta na multiplicação e depuração da informação. Nisso se baseia o conceito de inferential relational retrieval, técnica que permite o recolhimento de dados dispersos e desconexos, sistematizando-os de forma a criar um perfil de comportamento de indivíduo qualquer. O cruzamento dos registros torna possível que os bancos de dados – formados geralmente por muitas bases e por inúmeros dados – multipliquem-se, o mesmo acontecendo em relação aos critérios de classificação da informação. Essa facilitação das técnicas de captura, armazenamento e processamento da informação sofre um impulso ainda mais vertiginoso com a telemática, que vem adicionar um elemento novo a esse cenário, ao permitir o acesso à informação (arquivada em banco de dados) à distância. Os bancos de dados informatizados começam a se interligar; redes de computadores passam a fazer o trabalho que máquinas isoladas não conseguiam realizar. Mas as facilidades que a telemática oferece na transmissão de dados à distância traz consigo o outro lado de moeda: o risco da informação difundir-se de forma aleatória e incontrolada, atentando contra a privacidade das pessoas.



Essa nova realidade, como se disse, realça ainda mais a necessidade de se definir uma teoria da responsabilidade para os controladores e administradores de bancos de dados. A construção doutrinária de tal teoria não pode, é certo, ser de tal forma a impedir o desenvolvimento dos sistemas informáticos de coleta e armazenamento de dados. Os enormes benefícios que proporcionam não podem ser obscurecidos pela necessidade de regulamentação do uso de dados pessoais. Informação é um bem indispensável para a tomada de decisões. Além disso, exceções ao direito à privacidade podem ser ditadas por interesses outros, de caráter coletivo, como a liberdade de informação e de imprensa e a livre circulação de idéias. O que se deve buscar é um justo balanceamento entre o tratamento da informação e a preservação da privacidade individual. Por isso, a responsabilidade pela utilização de dados pessoais armazenados em bancos de dados deve atender a uma espécie de graduação, que irá variar dependendo da classe dos dados armazenados e da natureza da entidade que mantém o controle sobre eles. A manutenção de um determinado banco de dados pelo Poder Público, em atenção a finalidades de interesse público, pode presumir a legitimidade da coleta e utilização de dados pessoais, mesmo sem autorização da pessoa a quem eles se referem. Por outro lado, o recolhimento de dados que não estejam relacionados com aspectos particulares da vida de uma pessoa, naquilo que ela tem de mais íntimo, pode ser considerado como uma atividade livre ou sujeita a regras menos rígidas (em relação à outra categoria de dados – os dados sensíveis). Portanto, antes de tecermos algumas considerações sobre a responsabilidade do controlador de um banco de dados, é indispensável fazer uma distinção entre os tipos de dados que podem ser armazenados.

Classes de dados

Os dados passíveis de coleta e armazenamento em um banco de dados podem ser distinguidos em:

1- *Nominativos* – referem-se a alguma pessoa, quer seja física ou jurídica, e, por isso mesmo, em princípio pertencem à própria pessoa a que se referem. Os dados nominativos subdividem-se em:

a) *dados não sensíveis* – trata-se de categoria de dados nominativos que podem ser considerados como pertencentes ao domínio público e suscetíveis de apropriação por qualquer pessoa. Alguns dados que se referem a atributos da pessoa (como nome, estado civil e domicílio) ou a qualquer outra circunstância de sua vida civil e profissional (como profissão, ocupação, educação, filiação a grupos associativos etc.) em princípio podem ser armazenados e utilizados sem gerar danos ou riscos de danos às pessoas a quem se referem. Essa é uma característica definidora dos dados não sensíveis: são suscetíveis de apropriação por qualquer um, sem gerar danos ou riscos de danos.

Os direitos que se devem reconhecer à pessoa a quem se referem os dados não sensíveis se limitam ao controle de sua existência, sua veracidade e retificação, em caso de errônea. Os dados nominativos representam circunstâncias da vida das pessoas em momentos determinados. O transcurso de tempo pode afetar a correlação entre a circunstância da vida de uma pessoa e o seu respectivo registro existente em um determinado banco de dados, tornando-o irreal e desconexo.

Dessa forma, dados nominativos (não sensíveis) assumem a potencialidade de causar danos ou riscos de



danos às pessoas. Se em forma isolada não são suscetíveis de gerar danos ou riscos de danos, a sua justaposição ou desconexão com um correlato temporal ou fático faz com que assumam essa potencialidade. Como consequência, deve-se reconhecer à pessoa a quem os dados estão relacionados a faculdade de retificá-los, atualizá-los e aclará-los.

Como diz Salvador Bergel, deve reconhecer-se ao indivíduo, em relação a bancos de dados, determinados direitos que poderiam resumir-se a: um direito de acesso ao banco de dados, um direito de cancelamento da informação nele contida, um direito de conhecer se foi transmitida a terceiros, um direito de retificação, um direito de inserção e um direito de que a informação recolhida não seja mantida por tempo superior ao fim proposto .

Quando errôneas, a divulgação de informações contidas em uma base de dados nominativos (não sensíveis) pode gerar danos tanto às pessoas físicas às quais se referem como às pessoas jurídicas que eventualmente integrem. Por exemplo, a difusão de um dado desatualizado referente à uma anotação do cartório de imóveis pode impedir a outorga de um crédito, frustrando uma operação comercial e produzindo, conseqüentemente, dano à pessoa jurídica interessada no negócio e seus sócios.

b) *dados sensíveis* – outra categoria de dados nominativos estreitamente ligados à esfera de privacidade das pessoas. São dados que explicitam, por exemplo, as preferências sexuais da pessoa, as condições de sua saúde e características genéticas, sua adesão a idéias políticas, ideologias, crenças religiosas, bem como suas manias, traços do seu caráter e personalidade. Como seu armazenamento e uso não autorizados invadem a esfera íntima da pessoa, devem gozar de maior proteção jurídica do que outros dados nominativos (não sensíveis). Podem ser considerados bens privados, não suscetíveis de apropriação por qualquer outra pessoa que não aquela a que se referem.

Os direitos que se devem reconhecer à pessoa a quem se referem os dados sensíveis são mais amplos. Aos “proprietários” dos dados deve ser garantido não somente o direito de completá-los, aclará-los e retificá-los, mas mesmo o de proibir o seu uso.

Esse direito de exclusividade ou de limitação do uso dos dados, que deve ser conferido ao “titular” (a pessoa a qual se relacionam), surge em razão de que a divulgação de dados sensíveis sem seu consentimento pode afetar sua intimidade – direito que é protegido constitucionalmente, diga-se (art. 5º, X, da CF).

2- *Não nominativos* – são aqueles não relacionados a pessoas e que podem ser objeto de apropriação sem qualquer tipo de restrição, salvo algumas limitações decorrentes de regimes legais específicos – como as normas protetivas da propriedade intelectual, que impedem, p. ex., que sem autorização do autor alguém tenha acesso a um software e os dados nele contidos. São dados estatísticos, bibliográficos, econômicos, sociais, políticos e eleitorais não relacionados ou identificados – pelo menos diretamente – com alguma pessoa.

A apropriação, difusão ou utilização indevida de dados não nominativos em geral não atinge a órbita dos direitos da personalidade; como não se referem a dados pessoais, em regra sua manipulação não invade a intimidade ou privacidade dos indivíduos. As apropriações ilegítimas dessa categoria de dados costumam acarretar danos patrimoniais ao titular do direito, como acontece em relação a segredos



industriais, militares e políticos. Como esses dados são suscetíveis de valor econômico, a simples utilização sem autorização daquele que tem o direito de uso e acesso exclusivo sobre eles pode configurar o cometimento de um delito.

A difusão errônea de dados registrados em bancos de dados não nominativos pode gerar danos de distinta índole. Por exemplo, a divulgação de dados estatísticos incorretos, levando a projeções econômicas e sociais equivocadas e tomados como base para uma decisão política e de governo, pode repercutir sobre as pessoas objeto da pesquisa e, assim, gerar responsabilidade.

Classificação dos bancos de dados

De acordo com o tipo de dados armazenados, os bancos de dados podem se classificar em:

- a) bancos de dados nominativos (sensíveis e não sensíveis) de pessoas físicas;
- b) bancos de dados nominativos de pessoas jurídicas; e
- c) bancos de dados não nominativos.

Em relação à titularidade, os bancos de dados dividem-se em:

- a) bancos de dados administrados por pessoas físicas ou entidades privadas; e
- b) bancos de dados administrados por entidades públicas em geral, no qual se incluem os bancos de dados públicos em sentido amplo, a exemplo daqueles sob a administração de empresas privadas a serviço de um fim público e que, portanto, adquirem um caráter público.

Conclusões

A análise da responsabilidade do controlador de um banco de dados deve levar em consideração o que acima foi investigado, quanto à classificação dos dados e finalidades das bases de dados organizadas. Se a base de dados, por exemplo, está integrada somente por dados não sensíveis, os quais, como se disse, são do domínio público e suscetíveis de apropriação indiscriminada, a responsabilidade do operador – no caso de erro decorrente da justaposição ou desconexão temporal dos dados – deverá ser analisada em cada caso, segundo um padrão de subjetividade, isto é, de acordo com seu grau de culpa no episódio danoso. Se, por outro lado, a base de dados comporta dados sensíveis, pertencentes unicamente à esfera privada do indivíduo (a quem eles se referem) e conseqüentemente não suscetíveis de apropriação indistinta, a responsabilidade do operador, em princípio, enquadra-se dentro do âmbito da responsabilidade objetiva. Da mesma forma, a investigação da responsabilidade do operador deve ter em conta as finalidades para as quais uma base ou banco de dados é construída. Dependendo de seus fins, os dados coletados podem ser considerados como obtidos com ou sem conhecimento do titular (a pessoa a quem se referem). Uma base de dados erigida em atenção a um fim público qualquer e mantida por uma entidade pública goza da presunção de legitimidade no recolhimento dos informes, isto é, estes podem ser considerados como se tivessem sido recolhidos com o consentimento do titular. Essa presunção



decorre da constatação de que o direito à privacidade, de fundamento constitucional, pode ceder ante outros interesses também protegidos constitucionalmente, como o direito à saúde e segurança públicas. A criação e manutenção de certas bases de dados sensíveis podem resultar de vital importância para o interesse geral da coletividade.

A existência (ou não) de consentimento prévio ao recolhimento de dados pessoais é realmente determinante para a responsabilização do controlador. Partindo dessa circunstância, pode-se apontar as seguintes premissas para a construção de uma teoria da responsabilidade :

a) no uso de dados nominativos sensíveis, obtidos com o consentimento da pessoa a quem se referem, o controlador da base de dados responde pelos danos que sua atividade possa acarretar de forma objetiva. Para eximir-se da responsabilidade pelos danos, deverá demonstrar que de sua parte não houve culpa. Por exemplo, para o caso de invasão da base de dados por terceiros deverá demonstrar que as medidas de segurança e os cuidados técnicos que normalmente seriam suficientes para garantir a intangibilidade dos dados contidos na base.

b) no uso de dados nominativos sensíveis, obtidos sem o consentimento (ou obtidos com o consentimento mas mantidos em desatenção aos fins para os quais foi criada a base de dados) da pessoa, o controlador responde pelos danos objetivamente. Para eximir-se da responsabilidade pelos danos, é obrigado a demonstrar a culpa exclusiva da vítima ou de um terceiro que violou padrões de segurança e cuidados técnicos considerados suficientes para a garantia da intangibilidade dos dados.

c) no uso de dados nominativos não sensíveis, obtidos com o consentimento da pessoa, o controlador responde pelos danos com fundamento na culpa.

d) pelo uso errôneo de dados (desatualizados ou falsos) nominativos não sensíveis, obtidos com ou sem o consentimento da pessoa, o controlador da base responde objetivamente pelo risco da coisa.

Algumas dessas premissas, conforme expõe, podem sofrer alterações ou perder o valor segundo a relação de titularidade das bases, ou seja, conforme a entidade que coleta e armazena os dados, exercendo o controle sobre eles. De qualquer forma, fica observado que a responsabilidade pelo uso de dados nominativos varia segundo possam classificar-se em sensíveis ou não sensíveis e, ainda, tendo em vista a circunstância de a base de dados ser controlada por uma entidade pública ou privada, em atendimento a um fim público ou não.

No nosso país ainda não temos uma disciplina legal apropriada para a criação e manutenção de bases de dados sensíveis. É indispensável um maior rigor legal de modo a exercer um controle sobre empreendimentos informáticos que importem compilação e processamento de dados nominativos, que podem afetar direta ou indiretamente a privacidade das pessoas. O controle dessas atividades não pode impedir, é claro, o seu desenvolvimento, mas algumas exigências necessitam ser estabelecidas, no que tange a formalidades e requisitos técnicos para o funcionamento de bancos de dados públicos e privados. Além disso, as bases de dados sensíveis devem sofrer por parte da lei um maior resguardo, com a previsão de limitações temporais para sua conservação, objeções para transferência a terceiros, entre outras.

Date Created

07/06/2002