O CONTEXTO SOCIAL DO SURGIMENTO DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS

Gabriel Mendonça Hernandes

Mestre em Direito pela Escola Paulista de Direito
Pós-graduado em Direito Civil e Empresarial
Pós-graduado em Direito Digital e Compliance pela Faculdade Damásio IBMEC.
Atua na área de de Direito Civil, Família e Sucessões, Direito Digital e Direito Administrativo no escritório de advocacia Pellizzer & Hernandes - Assessoria Jurídica na cidade de Jundiaí - SP.

RESUMO

O presente trabalho abordará o surgimento das legislações de proteção de dados pelo mundo, especialmente na Europa, que foi pioneira na formação e desenvolvimento das tutelas de proteção de dados pessoais. O objetivo é demonstrar que a proteção de dados é tutelada a muito tempo em outros países e que a sua evolução ocorreu propriamente em torno da dinâmica em que o Estado e os particulares se comunicavam.

Palavras-chave: Proteção de Dados Pessoais. Princípio da Privacidade. Pessoa Natural. Historicidade.

INTRODUÇÃO

Com o surgimento do Estado Moderno (pós-guerra mundial) o Estado percebe a importância das informações pessoais de seus cidadãos para alavancar o crescimento coordenado e ordenado de toda uma nação.

O Estado com a intenção de realizar censos públicos, cuja finalidade é a formação de banco de dados com a intenção de monitorar e direcionar a expansão orgânica da população.

A desproporcionalidade na criação dos bancos de dados públicos motiva o avanço na criação de regulamentações das gerações de leis de proteção de dados pessoais.

Para melhor compreensão de como surgiu o movimento de legislações de proteção de dados, ou seja, sua origem, é fundamental o estudo de três casos históricos que se destacaram, são eles, *National Data Center, SAFARI e o* censo Alemão (autodeterminação informativa).

O caso *National Data Center* é a prova da absorção da tecnologia informática para processamento de dados pessoais e as tentativas para sua administração.

A ideia da implementação do *National Data Center* surgiu na intenção de uma estrutura administrativa simples (por volta de 1965), construir uma central integrada de armazenamento de informações pessoais que reuniria todas as informações de todos os cidadãos norte-americanos, captadas por todos os órgãos da administração federal, começando com a unificação dos dados do censo americano, fisco, registro trabalhista e previdência social.

Além do projeto de implantação do banco de dados único, a população americana, junto com o restante da população mundial, começava a conhecer os poderes do computador e da tecnologia que emergia a época.

A ideia de um banco de dados unificado buscava como principal solução a eficiência da administração pública norte-americana, o que motivou diversas medidas contrárias à sua criação, tanto do movimento do ludismo, como também por sociólogos que criticaram duramente a concentração de poder que o Estado passaria a ter frente aos cidadãos, totalmente contrária ao liberalismo defendido pelos americanos.

O sociólogo Vance Packard[1] foi uma das principais vozes a época:

> O maior risco em um banco de dados centralizado seria a possibilidade de colocar um poder tão grande nas mãos de pessoas que devem apertar alguns botões de computadores. Quando os detalhes das nossas vidas são armazenadas em um computador central ou em outros grandes sistemas de armazenamento, todos nós nos sujeitamos, em certa medida, ao controle exercido pelos operadores destas máquinas.

A concentração de informações pessoais em único banco de dados acaba por gerar maior eficiência de controle e gestão pela administração pública, posto que a localização da informação em

[1]Vance Packard. *"Don'tTell It To The Computer", The New York Times Magazine,* 08/01/1976, pp. 44 e ss. Apud SimsonGarfinkel, cit. p. 14 apud Doneda, Danilo. Da Privacidade à Proteção de Dados Pessoais, 2ª ed. São Paulo, Revista dos Tribunais, 2019.

um mesmo local agilizaria a pesquisa, bem como evitaria a duplicação de informações em banco de dados diversos.

Em que pese a eficiência do banco de dados, a proteção à privacidade dos titulares dos dados não era defendida pelos gestores públicos, surgindo assim as eventuais violações.

O Congresso norte-americano defendeu que a principal preocupação dos idealizadores do banco de dados tem que ser com a privacidade das informações pessoais dos cidadãos, conforme extraímos de suas recomendações finais[2]:

> (...)nada seja feito para estabelecer um banco de dados nacional sem que a proteção da privacidade seja observada e garantida ao máximo nível possível para os cidadãos de cuja informações pessoais seja formado o banco de dados.

Ao que se analisou, o banco de dados descentralizado demonstrou ser a melhor opção para a proteção de dados do titular, ou seja, é o emprego de uma arquitetura de informações pessoais distribuídas e não centralizadas no intuito de preservar as informações coletadas.

A polêmica em torno do *National Data Center* foi fundamental para entender a importância de uma arquitetura da estrutura informacional, como bem diz Danilo Doneda[3]:

---

[2]*The computerandinvasionofprivacy. SubcommitteeofthecomitteeongovernmentoperationHouseofRepresentatives. U.S. GovernmentPrinting Office: Washington, 1966, p.6*

[3]DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais, 2ª ed. São Paulo, Revista dos Tribunais, 2019

> (...)Esta relevância de uma determinada técnica de armazenamento de informações leva à constatação da importância da arquitetura da estrutura informacional que, em uma leitura conservadora da *privacy*no direito norte-americano, parecia mesmo se demonstrar legítima e não necessariamente invasiva; por outro lado, exibia uma potencial ameaça (theassaultonprivacy) à privacidade capaz de mudar a própria compreensão da *privacy*pelo ordenamento jurídico norte-americano.

O resultado da controvérsia no congresso foi o encerramento do projeto de unificação dos bancos de dados americanos, porém, em que pese a vitória dos que defendiam o direito à privacidade dos cidadãos, o congresso norte-americano não regulamentou a lei de proteção de dados naquela ocasião, sequer foi mencionado a sua relevância.

A ausência de regulamentação nos Estados Unidos, especificamente nos anos 70, embora tenha impedido o surgimento de um banco de dados unificado, prejudicou os cidadãos ao deixá-los vulneráveis, bem como por não ter vedado a coleta massiva de informações.

A exemplo dos Estados Unidos, na França não foi diferente, o *Institut National de la Statisti que* sob o mesmo pretexto dos órgãos americanos, propôs o denominado *SAFARI – Système Automastis é Pourles Fichiers Administratifs et le Réperoir edes Individus,* que era a informatização dos dados dos cidadãos em poder da administração pública francesa, por meio do número de seguridade social.

Acompanhando a justificativa norte-americana, a ideia era a centralização de um banco de dados para gerar maior eficiência para a administração pública, porém, sem nenhuma análise jurídica a respeito dos direitos a personalidade dos cidadãos, qual seja, o da privacidade e proteção de dados.

O projeto então apresentado pelo governo francês teve uma repercussão bastante negativa o que gerou uma atitude desesperada do primeiro ministro que determinou qualquer tipo de comunicação de dados entre os ministérios, ensejando o encerramento do projeto SAFARI.

Com o fracasso do projeto SAFARI, foi criada a comissão intitulada *Informatique et Libertés,* cujo trabalho resultou a lei francesa de proteção de dados de 1978, conhecida como *LoiInformatique, Fichiers et Libertés.*

Na Alemanha a situação foi diferente, posto que já existia uma cultura de proteção de dados no país, sendo o primeiro a tratar do assunto por meio de legislação (lei do *Land de* Hesse de 1970) e, em 1977, a lei de proteção de dados denominada *Bundesdatenchutzgetez.*

Os Estados alemães já possuíam em seus órgãos estruturas administrativas de proteção aos dados pessoais dos cidadãos, diferentemente de outros países no mundo, inclusive dentro da própria Europa.

A título de exemplo, é possível citar a legislação brasileira, Lei 13.709/2018, denominada como Lei Geral de Proteção de Dados Pessoais, que mesmo vigente, ainda depende de batalhas internas políticas e de lobby de grandes empresas.

O ponto crítico na Alemanha foi a demora para a produção de seu censo, provocando a desconfiança de vários setores da sociedade em relação ao método de coleta de informações utilizado e pelo seu destino a ser dado para estas.

O censo de 1982 foi previsto em legislação que determinava que cada cidadão deveria responder 160 perguntas, a serem posteriormente submetidas a tratamento informatizado[4], sendo que o cidadão que não respondesse estaria sujeito a uma multa considerável, o Estado poderia trocar informações sem anuência do titular dos dados e os registros civis (caso estivessem errados) seriam retificados com base no cruzamento das respostas.

O censo deu ensejo a uma sentença da Corte Constitucional Alemã (que se tornou referência quando o assunto é proteção de dados), promovida pelo ajuizamento de processo por comissionários de proteção de dados pessoais e entidades da sociedade civil.

A polêmica lei do censo alemão de 1982, além dos problemas já apresentados, também foi soberana no caso de conflitos com a então lei de proteção de dados pessoais alemã, conforme decidiu um juiz administrativo.

Além disso, em que pese a vigência da lei de proteção de dados pessoais, esta foi incapaz de proteger o titular de dados, uma vez que a finalidade, então pretendida pelo governo, era inalcançável frente a tantas informações requeridas no questionário.

Nas palavras de Danilo Doneda:

---

[4]DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais, 2ª ed. São Paulo, Revista dos Tribunais, 2019

> Vários foram os motivos que levaram a Corte a reconhecer esta profunda incompatibilidade. Um deles foi a observação de que, caso os dados recolhidos fossem utilizados ao mesmo tempo para fins administrativos e estatísticos (como na hipótese da retificação do registro civil a partir de dados de censo), estaria caracterizada a diversidade de finalidades, que impediria que o cidadão conhecesse o uso efetivo que seria feito de suas informações. Estas duas finalidades eram, além do mais, inconciliáveis, dado que o rigor estatístico não poderia coexistir com a necessidade dos órgãos administrativos de identificar os titulares destes dados. O tribunal, desta forma, reconheceu a necessidade de se observar o princípio da finalidade na coleta de dados pessoais.

Nos anos 70, em meio ao surgimento das legislações de proteção de dados na Europa e nos Estados Unidos, nota-se que a principal discussão era em torno da finalidade que o operador daria aos dados coletados, bem como, se havia consentimento e ciência por parte do titular para a coleta e tratamento de seus dados pessoais.

Os dados pessoais ganharam força após a Segunda Guerra Mundial e sua principal função era servir ao Estado como forma de dimensionar e acompanhar o desenvolvimento social de toda a população.

Ocorre que o uso desproporcional e a coleta massiva levou a situações como no caso da sentença alemã, que dentre a polêmica da finalidade da coleta dos dados, também foi fundamental para determinar que não importam quais dados são coletados, pois todos são relevantes para a proteção da privacidade do titular.

A sentença alemã foi pioneira ao tratar da relevância de qualquer dado, independentemente de juízo de valor ou importância, de modo que um dado isolado quando processado automaticamente gerará danos diretos ao seu titular.

Em se tratando do titular de dados, a sentença alemã apresentou a definição de "autodeterminação informativa", expressão já utilizada pelo direito norte-americano[5], que é a capacidade dos titulares de dados decidirem a forma, o momento e quais os limites para utilização de seus dados.

A autodeterminação informacional ganhou grande expressão na Europa nos anos 70, especialmente com a sentença alemã mencionada anteriormente, mas também no desenvolvimento e evolução das próprias legislações de proteção de dados, conforme notamos atualmente com a GDPR (*General Data Protecion*).

No Brasil, a autodeterminação informacional também é fundamental para a coleta e tratamento de dados, com previsão na LGPD no art. 2º, II[6], e também no art. 7º, I[7] na forma de consentimento.

GERAÇÕES DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS

A evolução das leis gerais de proteção de dados pessoais no mundo e, especialmente, na Europa, se deu justamente com base

[5]Alan Westin. *Privacyandfreedom* apud Doneda, Danilo. Da Privacidade à Proteção de Dados Pessoais, 2ª ed. São Paulo, Revista dos Tribunais, 2019.
[6]*Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:*
II - a autodeterminação informativa;
[7]*Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
I - mediante o fornecimento de consentimento pelo titular;

no preceito da autodeterminação informacional, na finalidade e no histórico de exploração de dados pelo poder público.

Nesse sentido, a primeira geração de leis de proteção de dados, conforme os exemplos já apresentados, surge com o processamento de dados massivos pelo Estado em prol de seu desenvolvimento, cujo o principal foco era a tecnologia em si, ou seja, o problema aparentemente era gerado pela gestão da tecnologia que deveria servir ao Estado democrático e não ao Estado totalitário.

Neste período, as legislações de proteção de dados foram editadas na intenção de evitar a figura do "Grande Irmão (Big Brother)" termo utilizado por Arthur Miller[8], em referência ao romance intitulado 1984 (George Orwell), em que a ideia central é de que o Estado monitora tudo e todos.

O *National Data Center* e o *SAFARI* são exemplos da figura do "grande irmão" e da concentração de banco de dados unificados e geridos pela autoridade estatal, sendo que a sua principal intenção é a de processar os dados conforme o desenvolvimento social de seus cidadãos.

Com o fim da centralização, principalmente após as decisões políticas de encerramento das atividades frente a insatisfação da população, os bancos de dados antes concentrados, passam a ser descentralizados e diluídos em diversos bancos de dados menores, caracterizando a segunda geração de leis de proteção de dados pessoais.

---

[8]MILLER, Arthur. *The assaultprivacy: computers, data banks, and dossiers*. apud BIONI, Bruno Ricardo, Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forens, 2019. p. 114

A atitude, até então política, ganhou outros contornos com o processamento de dados de forma descentralizada, ensejando a expansão da exploração dos dados por pessoas jurídicas privadas.

Já a segunda geração de leis de proteção de dados possui sua preocupação na descentralização dos bancos de dados, até então unificados, e com exploração pela pessoa jurídica privada, além da ramificação de banco de dados pela administração pública.

A geração de leis de proteção de dados pessoais passa a ter enfoque em direitos inerentes a pessoa e já conhecidos, como o direito à privacidade e o direito a personalidade, porém, não dispõe sobre os procedimentos tomados pelos encarregados no tratamento de dados pessoais, tratando de um direito então, meramente subjetivo.

Nessa geração de leis de proteção de dados pessoais, os bancos de dados unificados, são ramificados e administrados por empresas privadas, obriga os titulares dos dados a utilizarem seus direitos fundamentais como proteção, mais especificamente o direito à informação.

O consentimento ganha destaque na segunda geração de leis de proteção de dados, justamente baseado em direitos constitucionais, como o direito à informação. São exemplos de legislações, as leis da Áustria, da França, da Dinamarca e da Noruega.

O cidadão depende do fornecimento de determinadas informações para a sociabilidade, assim, sem o fornecimento de dados não será possível praticar atos comuns como realizar uma

compra, efetuar um pagamento, receber benefícios governamentais e até mesmo se entreter.

Neste sentido, Viktor Mayer-schönberger[9] trata sobre o custo social que o titular de dados sofre quanto às suas informações pessoais:

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas?"

A segunda geração de leis de proteção de dados permite que o titular defenda seus interesses como detentor de suas informações, mas evidencia a falta de preparo do próprio titular na tomada de decisão de suas próprias informações.

Nesse cenário, a terceira geração de proteção de dados ganha destaque no instante que transfere ao titular dos dados o poder de outorga da coleta e tratamento de seus dados pessoais, sendo este o único responsável pelo consentimento do uso de seus dados pessoais por parte da autoridade pública e das empresas privadas.

Como marco da terceira geração de leis de proteção de dados, tem-se o caso, já mencionado, do censo alemão de 1982,

---

[9]MAYER-SCHONBERGUER, Viktor. Generational develomp mente of data protection in Europe, Viktor Mayer-schönberger apud Mendes, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 41

em que a corte alemã entendeu como inconstitucional uma parte da legislação que não garantia o direito fundamental da autodeterminação informacional.

O titular dos dados ganha uma interpretação mais rigorosa sobre autodeterminação informativa, caracterizando verdadeiramente o protagonismo do titular em face dos controladores dos dados coletados e tratados.

A terceira geração garantem a participação do titular da coleta de seus dados até o compartilhamento, garantindo ciência de tudo que é feito com as informações durante o tratamento pelo controlador.

É importante destacarmos que a terceira geração de leis de proteção de dados, por volta dos anos 80, sofre grande impacto do surgimento de novas tecnologias informáticas, a capacidade e a velocidade de processamento de dados são enfatizadas e não é mais possível a localização física de banco de dados em centrais de processamento, posto que esses passam a ser armazenados em redes e podem ser transferidos em segundos.

A terceira geração de leis de proteção de dados serviu como adequação imediata à segunda geração de leis, na tentativa de conferir ao titular total autonomia na administração de seus dados, carecendo da outorga de consentimento em todas as fases de tratamento de dados.

A quarta geração de leis de proteção de dados pessoais tem o condão de corrigir a problemática em face da outorga de consentimento pelo titular dos dados.

O inegável *trade-off* entre fornecer ou não seus dados e, consequentemente, ter ou não acesso a bens e serviços, somados à vedação da utilização do direito à privacidade, obriga o titular de dados a se submeter, sendo que em caso de violação aos seus direitos à privacidade, não seria possível questionar, uma vez que aceitou os termos impostos pelo controlador.

A quarta geração de leis de proteção de dados busca resolver esses problemas em duas etapas. Primeiro, as legislações deram maior força para os titulares que se fortaleceram e passaram a ter um autocontrole maior sobre seus dados pessoais. Em segundo, algumas legislações tiraram a autonomia do titular de dados para determinados assuntos, justamente pela relevância e segurança jurídica que carece tal análise, como por exemplo, os dados sensíveis.

Em diversos países, especialmente na Europa, a quarta geração de leis de proteção de dados acarretou na promulgação de novas leis especiais, que regulamentam a norma geral, ou seja, as leis setoriais ampliam a proteção ao titular de dados, abrangendo os mais diversos ramos de informações coletadas e tratadas.

Cumpre destacar a crítica de Bruno Bioni[10] sobre a quarta geração:

> Ao mesmo tempo, contudo, esse progresso geracional não eliminou o protagonismo do consentimento. A sua centralidade permaneceu sendo o processo evolutivo, o consentimento passou a ser adjetivado, como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como ocorreu, portanto, no direito comunitário europeu. Essa

[10]BIONI, Bruno Ricardo, Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forens, 2019. p. 117

> distribuição de qualificadores acaba, portanto, por desdenhar um movimento refratário em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional.

Em que pese as evoluções das legislações de proteção de dados pelo mundo, o consentimento não perde seu *status* de foco central, o que deve ser analisado e criticado conforme cada operação de coleta e tratamento de dados.

É inerente ao titular de dados a posição de hipossuficiência, que mesmo com as evoluções legais do direito a proteção de dados, permanece como um dos principais fatores no tratamento de dados.

Notamos esse comportamento na própria legislação nacional, que em seus primeiros projetos apresentados no Congresso Nacional o protagonismo do titular era a única forma legítima para coleta e tratamento de dados pessoais, o que não se sustentou na legislação atual.

A atual lei geral de proteção de dados pessoais apresenta dez hipóteses de tratamento de dados pessoais (art. 7º), porém, colocando em seu primeiro inciso o “consentimento do titular” o que gerou discussões jurídicas sobre eventuais hierarquias entre os permissivos.

Em que pese a disposição hierárquica na legislação, a lei cuidou de dispor sobre outras formas de tratamento de dados, justamente para mitigar a outorga do consentimento e dar mais autonomia para o controlador administrar a coleta e tratamento de dados pessoais do titular.

Um caso em especial marcou o mundo pela vulnerabilidade e chamou a atenção de diversos países, especialmente os subdesenvolvidos da importância de uma lei que regulamenta a proteção de dados.

O caso ficou conhecido como *wannacry* e tratou de um vírus *ransomware* que basicamente bloqueou o banco de dados de diversas empresas, hospitais, empresa de telefonia, órgãos governamentais e solicitou resgate para liberar o acesso, afetando mais de 200 mil computadores, 150 países em todo o mundo.

O *ransomware* criptografava os bancos de dados e pedia um resgate inicial de U$ 300,00, aumentando conforme a demora no pagamento da quantia, feita em criptomoedas, de modo que dificultou a rastreabilidade do pagamento.

Além do modo de ação dos criminosos, o que chamou a atenção foi o fato de que só foi possível o ataque em função de uma falha do sistema operacional, porém, sem atualização em diversos computadores.

Significa dizer que, por mais que agentes criminosos realizaram o “sequestro” dos bancos de dados, se deu por uma falha de uma empresa desenvolvedora de software.

O *wanna cry* chamou a atenção de todo o mundo em função da somatória de responsabilidades em face do ataque global.

Em primeiro lugar, o governo norte-americano por ter conhecimento da vulnerabilidade e não ter comunicado a Empresa de sistema, em segundo lugar a própria Empresa que deveria ter agido com zelo pela aplicação e não o fez e, por fim, a

responsabilidade das próprias vítimas e profissionais de Tecnologia da Informação.

O ataque cibernético global alertou diversas empresas que não possuíam sequer licença para utilização do programa operacional, utilizando réplica em seus computadores com o finco de gerar economia aos gastos de governança de TI.

Não obstante, chamou a atenção das empresas a falta de programas de *compliance*, comitês de segurança da informação e o dano que gerou a imagem e até mesmo financeiro que as empresas se sujeitaram.

CONCLUSÃO

O histórico normativo das leis de proteção de dados pessoais ganhou novos rumos com o evento o ataque cibernético global, acelerando projetos de leis no Brasil e especialmente a adequação das empresas, especialmente as multinacionais, as legislações estrangeiras.

Com as experiências nos países pelo mundo, as legislações de proteção de dados ganharam foco com as decorrentes violações aos princípios e direitos dos titulares de dados pessoais.

O surgimento das legislações começou com base na unificação de banco de dados pelos Estados e consequemente pela troca de informações entre órgãos internos sem a devida ciência da população.

No Brasil, a tutela da proteção de dados surgiu através de legislações setoriais e da adaptação de entendimentos da

legislação vigente à época, que só viu a sua regulamentação própria, com a vigência total da Lei Geral de Proteção de Dados Pessoais (LGPD).

REFERÊNCIAS BIBLIOGRÁFICAS

The computer and invasion of privacy. Subcommittee e of the comitte e on government operation. House of Representatives. U.S. Government Printing Office: Washington, 1966.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais, 2ª ed. São Paulo, Revista dos Tribunais, 2019

Alan Westin. *Privacy and freedom* apud Doneda, Danilo. Da Privacidade à Proteção de Dados Pessoais, 2ª ed. São Paulo, Revista dos Tribunais, 2019.

MILLER, Arthur. *The assault privacy: computers, data banks, and dossiers.* apud BIONI, Bruno Ricardo, Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forens, 2019.

BIONI, Bruno Ricardo, Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forens, 2019.

MAYER-SCHONBERGUER, Viktor. Generational develomp mente of data protection in Europe, Viktor Mayer-schönberger apud Mendes, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

Mendes, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014