Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais

Emilio Tissato Nakamura[1], José Reynaldo Formigoni Filho[1], Marcos Cesar Ide[1]

[1]CPQD
Rua Ricardo Benetton, 1000, Campinas, SP - Brasil
nakamura@cpqd.com.br, reynaldo@cpqd.com.br, mcide@cpqd.com.b

Abstract. *This paper presents the main aspects related to personal data, the development of general data protection laws, as well as the use of traditional information security framewoks for the protection of personal data. In addition, a risk assessment and security measures for personal data is presented to support companies to attend the security requirements demanded by the Brazilian General Data Protection Law.*

Resumo. *Este artigo trata de aspectos relacionados com a proteção de dados pessoais, da criação das leis gerais de proteção de dados, assim como quais são as alternativas que as empresas estão buscando para atender aos requisitos de segurança demandados por tais leis. Além disso, é apresentada uma metodologia de avaliação de risco e segurança para suportar as empresas no atendimento dos requisitos de segurança demandados pela Lei Geral de Proteção de Dados do Brasil (LGPD).*

1. Dados pessoais e sua proteção

A utilização massiva de dados pessoais ocorreu a partir de meados do século passado em razão da burocratização dos setores públicos e privados e do desenvolvimento das tecnologias de informação e comunicação [Bennet, 1992]. Tal desenvolvimento aumentou o fluxo de dados entre pessoas utilizando dispositivos fixos e móveis e, mais recentemente, com o advento da Internet das Coisas (IoT), entre pessoas e coisas e entre diferentes dispositivos.

Existem várias definições e conceitos associados aos dados pessoais. O Regulamento Geral de Proteção de Dados (*General Data Protection Regulation,* GDPR) da União Europeia define dados pessoais, em seu artigo 4º. como [GDPR, 2016]: "informação relativa a uma pessoa natural identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa natural que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural;".

No seu artigo 5º., a Lei Geral de Proteção de Dados Pessoais [LGPD, 2018] brasileira define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável".

O que é a proteção de dados pessoais? Segundo [Mendes, 2014], “a disciplina da proteção de dados pessoais emerge no âmbito da sociedade da informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados em si, mas a pessoa que é titular desses dados”.

2. As Leis gerais de Proteção de Dados Pessoais

Vários países adotaram um modelo jurídico para proteção de dados pessoais com a adoção de um regime legal de proteção de dados, na forma de uma lei geral. As leis gerais de proteção de dados pessoais se firmaram com um dos mecanismos mais eficazes de se proteger a privacidade nos países desenvolvidos. Com exceção dos Estados Unidos, a maioria dos países desenvolvidos, assim como o Brasil, aprovaram leis abrangentes contemplando os setores públicos e privado. Embora alguns países tenham suas leis gerais de proteção de dados, estas podem coexistir com normas setoriais, regulando setores específicos de forma complementar às leis gerais.

a) Regulamento Geral de Proteção de Dados da União Europeia

O Regulamento Geral de Proteção de Dados da União Europeia [GDPR, 2016] foi elaborado pelo Parlamento Europeu e Conselho da União Europeia, sendo publicado no dia 04 de maio de 2016. Ele foi implementado nos 28 países membros da União Europeia em 25 de maio de 2018. O regulamento, que na União Europeia tem força de lei, possui um conteúdo bastante extenso, com 173 considerandos e 99 artigos. A implantação do regulamento não impede que o país possa também ter leis setoriais específicas, se o assunto demandar.

Segundo [Lima, 2018], “o foco é a proteção de direitos e garantias fundamentais dos cidadãos, com o objetivo de mitigar os riscos, em relação ao que pode ser feito, a partir da coleta e do futuro uso, compartilhamento, armazenamento, entre outros, desses dados”.

b) Lei Geral de Proteção de Dados Pessoais

A Lei 13.709/2018, também conhecida como Lei Geral de Proteção de Dados brasileira [LGPD, 2018], foi publicada em 14 de agosto de 2018 e, segundo [Cots, 2018], com esta publicação “o Brasil se integrou, não sem um certo atraso, ao grupo de países que possuem legislações específicas para proteção de dados pessoais”. Pode-se afirmar que a grande fonte de inspiração para a elaboração da LGPD foi o GDPR, sendo a primeira mais genérica e, consequentemente, menos detalhada que o regulamento.

Com a Medida Provisória Nº 869, de 27 de dezembro de 2018, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. Vale destacar que as leis setoriais permanecerão coexistindo com a LGPD. Na visão de [Lima, 2018], a Autoridade Nacional de Proteção de Dados e o Poder Judiciário deverão ter forte atuação para, diante de cada caso concreto, optar sobre qual a melhor legislação a ser aplicada.

Na data de aprovação da LGPD, estabeleceu-se um prazo de 18 meses para que as empresas pudessem se adequar aos requisitos demandados pela lei.

3. Os Padrões de Segurança Corporativos e a Proteção de Dados Pessoais

Uma das formas das empresas que trabalham com dados pessoais se adequarem aos requisitos gerados pelas leis gerais de proteção de dados é fazendo uso, com as devidas adaptações, dos frameworks ou padrões de segurança existentes, principalmente se a empresa já faz uso de algum destes.

Um dos frameworks mais utilizados são as normas da família ISO 27000. Estas normas tratam da implementação de um Sistema de Gestão de Segurança da Informação (SGSI), sendo que mais conhecidas são a ISO 27001 [ABNT NBR ISO 27001, 2006], que descreve um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI e a ISO 27002 [ABNT NBR ISO 27002, 2005], que oferece objetivos de controles de segurança, que serão implementados pelos responsáveis pelo SGSI, dependendo da aplicabilidade e resultados da análise de riscos e também dos requisitos de segurança identificados naquele contexto.

Muitas empresas têm adotado a ISO 27000 como framework para a segurança da informação, porém a sua implementação, de forma isolada, não garante o integral atendimento às leis gerais de proteção de dados. Fundamentalmente, a família de normas 27000 trata de proteção de informações do ponto de vista da entidade que está implementando o SGSI e não do ponto de vista dos direitos dos indivíduos. É claro que ao proteger as informações da organização, as informações das pessoas também estarão protegidas, porém alguns direitos estabelecidos na legislação não estão contemplados na norma, como por exemplo o direito de ter informações removidas e o consentimento do dono das informações. Algumas empresas disponibilizam tabelas onde é feito o mapeamento da ISO 27000 e GDPR [ISO 27K Forum, 2016]. Estima-se que cerca de 75 a 80% dos requisitos da GDPR estão contemplados pelo framework.

Outro padrão que também passa pelo processo da adaptação é o *Control Objectives for Information and related Technology* (COBIT), que foi lançado pela *Information Systems Audit and Control Association* (ISACA) em 1996 e está na quinta versão. Em 2017 a ISACA propôs um conjunto de procedimentos com os requisitos do GDPR utilizando como base o framework do COBIT [ISACA, 2017]. Os mesmos procedimentos poderiam ser utilizados na implementação dos requisitos da LGPD.

4. Metodologia de Gestão Risco para Proteção de Dados Pessoais

Neste item propõe-se uma metodologia para auxiliar as empresas na adequação aos requisitos demandados pela LGPD. A metodologia é composta por três fases principais que são baseadas em elementos fundamentais de segurança da informação, gestão de riscos e privacidade de dados. De uma forma integrada, eles visam identificar e avaliar os dados pessoais, os seus pontos de vazamento e os mecanismos de segurança, que são os objetos da LGPD.

4.1. Elementos Fundamentais

A metodologia de gestão de riscos para proteção de dados pessoais considera os seguintes elementos como fundamentais para a aderência das organizações na LGPD:

- Lista de ativos da organização, tais como sistemas (*Enterprise Resource Planning* (ERP), *Customer Relationship Management* (CRM), *Active Directory*

(AD), por exemplo), produtos e processos, dependendo do caso. O nível de granularidade também depende do tipo de análise em andamento;
- Quais dados são tratados pela organização e, destes, quais são dados pessoais;
- Quem insere e quem consome os dados;
- Quais os componentes (tecnológicos ou não) pelos quais os dados são processados, transmitidos ou armazenados;
- Quais os estados dos dados em cada um dos componentes: *Data-In-Use* (DIU) ou processados, *Data-In-Motion* (DIM) ou transmitidos; ou *Data-At-Rest* (DAR) ou armazenados;
- Quais artefatos de base legal e regulatória estão sendo utilizados, tais como termos de consentimento, declaração de contatos, declaração de mecanismos de segurança, entre outros;
- Quais os controles de segurança que estão sendo utilizados para proteger os dados pessoais, incluindo tecnologias e processos;
- Quais os pontos de potenciais vazamentos dos dados pessoais;
- Quais as ameaças que podem levar a incidentes de segurança;
- Quais os agentes de ameaça que podem explorar vulnerabilidades dos componentes;
- Quais vulnerabilidades que podem ser exploradas pelos agentes de ameaça;
- Quais os impactos relacionados à privacidade dos titulares dos dados;
- Quais as probabilidades de vazamentos de dados pessoais.

4.2. Fases da Metodologia

A metodologia é composta por três fases principais descritas a seguir.

a) Identificação do fluxo de dados pessoais

O fluxo de dados pessoais permite entender quais são os dados pessoais e cada um de seus estados (DIU, DIM, DAR) em todos os componentes, que por sua vez representam os pontos de ataques em que os vazamentos podem ocorrer. A metodologia adota o conceito de que há dois grandes conjuntos de necessidades relacionados à LGPD. O primeiro conjunto é a base legal e regulatória, que estabelece a forma de coleta dos dados pessoais, os relacionamentos necessários para o consentimento, que depende da forma como os dados são protegidos e gerenciados, incluindo o repasse para terceiros. Já o segundo conjunto diz respeito à possibilidade de vazamentos de dados pessoais, considerando o uso de controles de segurança que vão desde o desenvolvimento seguro até o gerenciamento de riscos, visando diminuir as vulnerabilidades.

b) Análise de gap e de riscos

Como não é possível aplicar todos os controles de segurança, tanto pela viabilidade quanto pela real necessidade, é preciso a realização de uma análise de gap e riscos, que analisa o fluxo de dados pessoais para estabelecer prioridades e justificativas para a implementação dos controles de segurança estritamente necessários para a proteção de dados pessoais específicos de cada organização. Ela envolve elementos como componentes, agentes de ameaça, ameaças, vulnerabilidades, probabilidades e impactos.

c) Estratégia de adequação à LGPD

A estratégia de adequação à lei é definida de acordo com os resultados da análise de gap e riscos, que por sua vez foi gerada a partir do fluxo de dados pessoais. É importante

salientar que há dados pessoais que são mais críticos do que outros, seja pela quantidade de dados quanto pela quantidade de usuários relacionados. Por exemplo, uma organização pode armazenar dados como endereço de e-mail e telefone enquanto outra pode armazenar dados que incluem nome, endereço, nome da mãe e número de RG. Em outro exemplo, uma organização pode ter estes dados pessoais apenas como cadastro de usuários que acessam determinados sistemas, enquanto outra organização pode ter estes dados que são utilizados em campanhas de marketing e atendimentos personalizados, com compartilhamento entre parceiros de negócios.

Além disso, caso dados de menores e adolescentes, ou daqueles considerados sensíveis forem coletados, a criticidade aumenta muito. Esta variabilidade entre dados pessoais faz com que a estratégia de proteção de dados pessoais seja diferente de uma organização para outra, o que reforça a importância do uso de uma metodologia específica que incorpore a gestão de riscos.

O framework de segurança e privacidade, fruto da aplicação da metodologia de gestão de riscos para proteção de dados pessoais, é composto por processos, tecnologias e mecanismos de proteção. Os processos devem envolver elementos como programa de privacidade, governança, cultura de privacidade e estruturação, enquanto as tecnologias envolvem a arquitetura de dados, anonimização e pseudonimização, além da criptografia. Já a proteção dos dados pessoais envolve gerenciamento de riscos, segurança da informação e operação e monitoramento.

Atualmente, a validação da metodologia está sendo realizada em uma organização com processos de diferentes naturezas, tais como desenvolvimento de produtos de softwares, projetos de inovação com desenvolvimento de tecnologias em software, firmware e hardware, assim como oferta de serviços especializados de consultoria para diferentes setores. Além do tratamento de dados pessoais para os processos internos, produtos e projetos de inovação também envolvem dados pessoais.

5. Conclusões

Com o advento da transformação digital, pode-se afirmar que a grande maioria das empresas, em pelo menos um dos seus processos operacionais, trata de dados pessoais. O esforço de adequação às leis gerais de proteção de dados costuma ser grande para as empresas, demandando tempo e investimento em pessoas, mudanças de processos, aquisição de ferramentas de segurança da informação e, em muitos casos, contratação de serviços especializados de consultoria e de segurança da informação, tais como testes de vulnerabilidade e análise de código, dentre outros. Tal adequação é um desafio ainda maior para as pequenas e médias empresas (PMEs), as quais costumam apresentar restrições orçamentárias e de fluxo de caixa. Em função disso, a ENISA lançou, em dezembro 2016, um relatório específico para auxiliar as PMEs da União Europeia na adequação ao GDPR [ENISA, 2016].

Para a grande maioria das empresas europeias, o processo de adequação ao GDPR ainda não foi finalizado, apesar da data limite ter sido março de 2018. Muitas delas iniciaram o processo tardiamente e outras decidiram, após uma análise de riscos, priorizar a implantação dos controles mais críticos. Pela movimentação incipiente até agora observada, é possível afirmar que movimento semelhante ocorrerá aqui no Brasil.

Para as empresas desenvolvedoras de softwares, um dos grandes desafios é a inclusão, nas metodologias de desenvolvimento, das abordagens *security-by-design* e *privacy-by-design*, considerando os aspectos da segurança dos dados pessoais e privacidade já nas primeiras etapas do desenvolvimento. Até o presente, muitas empresas relutaram em adotar tais abordagens em função de reflexos nos custos de desenvolvimento.

A metodologia está sendo aplicada em uma organização, devendo sofrer as tradicionais evoluções, principalmente considerando a variedade de setores da economia e também o tamanho das organizações, que refletem diretamente no tratamento de dados pessoais.

Referências bibliográficas

ABNT NBR ISO 27001:2006 - Tecnologia da informação - Técnicas para segurança - Sistemas de Gestão de Segurança da Informação – Requisitos.

ABNT NBR ISO 27002:2005 - Tecnologia da informação - Técnicas para segurança - Código de prática para a gestão de segurança da informação.

Cots, Márcio, Oliveira, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. Primeira edição. São Paulo: Thomson Reuters Brasil, 2018.

ENISA. Guidelines for SMEs on the security of personal data processing. Dezembro de 2016. Disponível em: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing. Acesso em: 15/06/2019.

ISACA. Key Tips & Takeaways for GDPR Implementation Using COBIT® 5. Disponível em: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Adopting-GDPR-Using-COBIT-5.aspx. Acesso em: 10/-6/2019.

ISO 27K Forum. Mapping between GDPR (EU General Data Protection Regulation) and ISO27k. Nov. 2016. Disponível em: https://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.docx. Acesso em: 21/06/2019.

LGPD. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21/06/2019.

Lima, C. C. Carvalho. Objeto, Aplicação material e Aplicação territorial. In: Maldonado, Viviane et al. Comentários ao GDPR – Regulamento Geral de Proteção de Dados da União Europeia. 1ª. ed. SP: Revista Tribunais/Thomson Reuters, 2018.

Mendes, L. Schertel. Privacidade e proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. 1ª. ed. São Paulo: Saraiva Educação, 2014.

GDPR. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 abril 2016. Tratamento de dados pessoais e livre circulação, que revoga a Diretiva 95/46/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 15/06/2019.