Ricardo César Gonçalves Sant'Ana
Moisés Lima Dutra
Guilherme Ataíde Dias
Organizadores

ANAIS
WIDaT 2018

Organização do WIDaT 2018

- **Organização Geral:**

  Guilherme Ataíde Dias (PPGCI-UFPB) - Coordenador geral do evento

  Moisés Lima Dutra (PPGCIN-UFSC) - Vice-coordenador

- **Coordenador da Comissão Científica:**

  Ricardo César Gonçalves Sant'Ana (PPGCI-UNESP)

- **Comissão científica**

  Adilson Luiz Pinto (PPGCIN-UFSC)

  Ana Alice Baptista (Universidade do Minho, Portugal)

  Ana Carolina Simionato (PPGCI-UFSCar)

  Angela Maria Grossi de Carvalho (PPGCI-UNESP)

  Bernardina Maria Juvenal Freire de Oliveira (PPGCI-UFPB)

  Cristian Berrío-Zapata (PPGCI-UFPA)

  Dalton Lopes Martins (FCI-UnB)

  Denysson Axel Ribeiro Mota (PPGB-UFCA)

  Douglas Dyllon Jeronimo de Macedo (PPGCIN-UFSC)

  Ed Porto Bezerra (PPGI-UFPB)

  Edgar Bisset Alvarez (PPGCIN-UFSC)

  Edna Gusmão de Goés Brennand (MPGOA-UFPB)

  Edna Gomes Pinheiro (DCI-UFPB)

  Elaine Parra Affonso (FATEC-SP)

  Elvis Fusco (UNIVEM-Marília)

  Enrique Muriel Torrado (PPGCIN-UFSC)

  Evandro de Barros Costa (IC-UFAL)

  Fábio Paraguaçu (IC-UFAL)

  Fernando de Assis Rodrigues (PPGCI-UNESP)

  Gustavo Medeiros de Araújo (PPGCIN-UFSC)

  Henry Pôncio Cruz de Oliveira (PPGCI-UFPB)

  Joana Coeli Ribeiro Garcia (PPGCI-UFPB)

  José Eduardo Santarém Segundo (USP-FFCLRP)

  Leonardo Castro Botega (UNIVEM-Marília)

  Luana Farias Sales Marques (PPGCI-IBICT-UFRJ)

  Marckson Roberto Ferreira de Sousa (PPGCI-UFPB)

  Luís Fernando Sayão (CNEN)

  Marcelo Morandini (EACH-USP)

  Márcio Matias (PPGCIN-UFSC)

  Marcos Mucheroni (CBD-USP)

  Marynice de Medeiros Matos Autran (PPGCI-UFPB)

Maurício Barcellos Almeida (PPGGOC-UFMG)
Moisés Lima Dutra (PPGCIN-UFSC)
Plácida Leopoldina V. da Costa Santos (PPGCI-UNESP)
Pedro Luiz Pizzigatti Corrêa (POLI-USP)
Renata Baracho (PPGGOC-UFMG)
Ricardo César Gonçalves Sant'Ana (PPGCI-UNESP)
Robson Rodrigues Lemos (UFSC-Araranguá)
Rogério Ramalho (PPGCI-UFSCar)
Ryan Ribeiro de Azevedo (UFRPE-UAG)
Sandra de Albuquerque Siebra (PPGCI-UFPE)
Sandro Rautenberg (DECOMP-UNICENTRO)
Silvana Aparecida Borsetti G. Vidotti (PPGCI-UNESP)
Virginia Bentes Pinto (PPGCI-UFC)
Wagner Junqueira de Araújo (PPGCI-UFPB)
Zaira Regina Zafalon (PPGCI-UFSCar)

- **Coordenador do Cerimonial:**
  André Luiz Dias de França (PPGCI-UFPB)

- **Coordenador da Equipe Técnica Local:**
  Laerte Pereira da Silva Júnior (CCHLA-UFPB)

- **Equipe Técnica Local:**
  Adriana Alves Rodrigues (PPGCI-UFPB)
  Antonio Felipe dos Santos (MPGOA-UFPB)
  Débora Gomes de Araújo (PPGCI-UFPB)
  Pedro Augusto de Lima Barroso (PPGCI-UFPB)
  Pollianna Marys de Souza e Silva (PPGCI-UFPB)
  Renata Lemos dos Anjos (PPGCI-UFPB)

DESAFIOS TECNOLÓGICOS NO PROCESSO DE RECEPÇÃO NORMATIVA: adequação e conformidade na perspectiva da Lei de Proteção de Dados Pessoais

TECHNOLOGICAL CHALLENGES IN THE NORMATIVE RECEPTION PROCESS: adequacy and compliance from the perspective of the Law of Protection of Personal Data

Andrea Carmo Name Willemin[1] Geralda Magella de Faria[2] Cláudio José Amante[3]
(1) Universidade Federal de Santa Catarina (UFSC), Programa de Pós-Graduação em Ciência da Informação, Centro de Ciências da Educação, Bloco B, sala 105, Campus Universitário, Trindade, Florianópolis, andrea.willemin@gmail.com
(2) Universidade Federal de Santa Catarina (UFSC), Programa de Pós-Graduação em Direito, Centro de Ciências Jurídica (CCJ), Campus Universitário, Trindade, Florianópolis, geraldamagella@gmail.com
(3) Universidade Federal de Santa Catarina (UFSC), Coordenador do Programa de Pós-Graduação em Administração Universitária, Professor do Departamento de Odontologia, Campus Administração Universitária, Trindade, Florianópolis, claudio020461@gmail.com

Resumo: (1) A Lei de Proteção de Dados, recém editada no Brasil, tem a marca de resguardar, proteger e cuidar dos dados – entendidos estes pertinentes à inovação e tecnologia, de cunho sensível, privado e pertinentes à pessoa - com a medida do zelo e da segurança que até então não foram reservados pela legislação. (2) A pesquisa levada a termo pretende ser exploratória, qualitativa e que terá como base uma proposta de resolução de problemas. (3) Neste sentido, a adequação tecnológica e organizacional requer a indicação de um "modelo de processo de resolução de problemas", cujo fundamento deve prestar ao regramento normativo, cumplicidade e conformidade até então inexistente. (4) Assim, processo na esfera de proteção de dados requer procedimentos que busquem inovação e configuração tecnológica apta ao desempenho seguro de dados pessoais.
Palavras-chave: Lei de Proteção de Dados Pessoais. Privacidade; Inovação. Política Nacional de Ciência, Tecnologia e Inovação.

Abstract: (1) The Data Protection Law, recently published in Brazil, has the mark of safeguarding, protecting and taking care of the data - understood as pertinent to innovation and technology, sensitive, private and pertinent to the person - with the measure of zeal and security that were not previously reserved by law. (2) The research carried out to term is intended to be exploratory, qualitative and based on a proposal for problem resolution. (3) In this sense, the technological and organizational adequacy requires the indication of a "problem resolution process model", the foundation of which should be to regulate law, complicity and compliance that did not exist until then. (4) Indeed, process in the sphere of data protection requires procedures that seek innovation and technological configuration for the safe performance of personal data.
Keywords: Law of Protection of Personal Data. Privacy. Innovation. National Policy on Science, Technology and Innovation.

1 INTRODUÇÃO E METODOLOGIA

Com os dados ganhando destaque e espaço na cena internacional e brasileira, saber interpretar e aplicar as diferentes leis que dispõe sobre Proteção de Dados Pessoais é essencial para atuar neste novo cenário regido pela confluência do universo jurídico e tecnológico. A GDPR, Lei Europeia de Proteção de Dados Pessoais, e a brasileira, no caso a Lei de Proteção de Dados Pessoais LPDP - Lei 13709, de 14 de agosto de 2018, possuem inúmeros desafios de caráter tecnológico e jurídico.

Vários pontos da lei chamam particularmente a atenção em razão do caráter inovador e desafiador que trarão quanto a sua integração nos diferentes sistemas de informação e organizacionais gerados pelas novas exigências legais. Várias nações regularam a proteção de dados pessoais há décadas atrás. Hoje, por exemplo, a Europa possui uma legislação forte que impõe diferentes metodologias nas quais a proteção de dados pessoais é pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais.

O Brasil aprovou recentemente sua Lei de Proteção de Dados Pessoais. Trabalhar com os dados pessoais agora exige especial desafio para que a proteção dispensada pela lei seja realizada sem que com isso se perca o caráter inovador e realizador buscado pelas novas tecnologias em desenvolvimento. Por inovação, entende-se a atividade de caráter científico, tecnológico, organizacional, financeiro ou comercial proposta e executada com o objetivo de obter produtos, processo tecnológico e serviços totalmente novos ou melhorados, que pode se dar em regime de transação comercial ou não. Inovação é definida como resultado da introdução de novo conhecimento ou tecnologia econômica e socialmente útil (o sentido do novo se aplica ao local onde é introduzido e não possui sentido universal). (BRASIL, 2018).

Para tanto é necessário criar processos que permitam as organizações integrarem dentro de suas estruturas as novas regras legais. Os desafios são inúmeros e em diferentes aspectos. A figura do apêndice A demonstra, de forma exemplificava, as três dimensões (organizacionais, tecnológicas e humanas) necessárias de figurarem de forma harmônica no sistema de informação possibilitando assim as soluções de negócios desejadas. Neste estudo serão levantados alguns dos desafios de dimensões tecnológicas impostos pela lei geral de proteção de dados pessoais que precisarão ser implantados nas diferentes organizações a partir de janeiro de 2020. A complexidade do desafio trazido pela LPDP exige num primeiro ponto que se identifique o que é necessário ser feito. Pois são muitas as novidades introduzidas pela lei e que passarão a ser cobradas. Assim sendo convém a apresentação às organizações de um panorama geral do que está sendo solicitado em termos de adaptações tecnológicas para que daí se estabeleçam processos de adequação das diferentes implementações exigidas pela lei.

No tocante aos procedimentos metodológicos do presente estudo, trata-se de uma pesquisa exploratória, que aborda certos desafios tecnológicos encontrados quando da integração com os novos dispositivos legais trazidos pela lei de proteção de dados pessoais. Da mesma forma pode ser entendida como uma pesquisa qualitativa e de natureza básica que terá como base o passo 01 (um) "modelo do processo de resolução de problemas" (LAUDON; LAUDON, 2014, p. 20).

2 OBJETIVOS

O objetivo geral deste estudo é identificar os desafios tecnológicos no processo de recepção normativa da Lei de Proteção de Dados Pessoais relacionando aos principais desafios de dimensões tecnológicas decorrentes da Lei 13709/2018, para a criação de um "modelo de processo de resolução de problemas" (LAUDON; LAUDON, 2014, p. 20).

Este estudo é a primeira etapa necessária para se "entender e solucionar problemas organizacionais por meio dos sistemas de informação" (Apêndice B), que poderá ser aplicado dentro das diferentes organizações que terão o desafio, até janeiro de 2020, de implantarem a nova Lei de Proteção de Dados Pessoais brasileira. Para que se possa resolver problemas, neste caso, particularmente os referentes as exigências legais, é necessário, primeiramente, que exista consenso sobre sua existência, suas causas e o que pode ser feito quanto a eles, levando-se em conta os recursos limitados que as organizações dispõe (LAUDON; LAUDON, 2014, p. 20) e a necessidade das organizações se adaptarem. A identificação de alguns dos desafios tecnológicos da Lei de Proteção de Dados Pessoais nos sistemas de informação poderá, com o auxílio da ferramenta do modelo de "processo de resolução de problemas" (Apêndice C) num primeiro plano, auxiliar a evidenciar os pontos que necessitam serem trabalhados, para que se possa, depois estabelecer diferentes propostas; avaliar e escolher as propostas e implantar as melhores soluções nas organizações públicas e privadas de forma a se cumprir as novas exigências tecnológicas impostas pela lei.

3 CIÊNCIA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Foi uma longa gestação, da pedra ao byte, e da descoberta e reconhecimento quanto a importância da seleção, arquivamento, transmissão e o próprio aprendizado, entre prática e teoria até dar o passo do reconhecimento da Ciência da Informação.

Na história humana, tudo começou com a oralidade, depois vieram os registros. Rudimentares aos olhos atuais, mas de significado incomensurável para a humanidade. Cita-se, o Cilindro de Ciro "o Grande", primeiro rei da Pérsia, que em 539 a.c conquistou a Babilonia, e recomendou o vetusto registro que é reconhecido como a 1ª. Carta de Direitos Humanos (BRASIL, 2018). Também a Pedra da Roseta, decifrada recentemente, entre 1802 a 1822, por Chanpollion, e sua inscrição registra um decreto do rei Ptolomeu V, promulgado em 196 a.C., na cidade Mênfis. É certo que o desejo político, no caso, a necessidade do registro e a transmissão às gerações fizeram de "dados" como este, e os milhares que se seguiram, uma qualidade e condição de seu armazenamento e transmissão, quer pelo trabalho, como também, pela própria necessidade humana de organização.

Os primeiros cientistas da informação, conforme revela Araújo (2018), tiveram reconhecimento somente no Século XX, de forma que de 1920 a 1940, da Inglaterra até aos EUA e em outros países, os cientistas puderam abastecer seus colegas - com os Science Services - em suas respectivas áreas de estudos, com índices, resumos, canais, arquivos. Assim, os "ex" químicos, físicos, engenheiros e outros cientistas alçaram a condição de cientistas da Informação, saíram da prática para o universo da institucionalização.

De forma concreta, em 1968, o American Documentation Institute, dos Estados Unidos, mudou seu nome para American Society for Information Science, tornando-se a primeira instituição de Ciência da Informação do mundo. Contribuíram também para sua formação, primeiro a Inglaterra, com a realização da Royal Society Scientific Information Conference, em 1948, e a criação, em 1958, do Institute of Information Scientist. Pouco depois, na União Soviética, foi criado o Viniti, Vserossiisky Institut Nauchnoi i Tekhnicheskoi Informatsii, vinculado à Academia de Ciências. E, a seguir, em 1958, ocorreu nos Estados Unidos a International Conference on Scientific Information, quando, a Ciência da Informação alça a condição de ciência dedicada à informação em ciência e tecnologia, com a preocupação de base dessas ações: não mais a necessidade de se ter a posse dos documentos, mas a prioridade dada à sua circulação, ao seu fluxo, e ao atendimento das necessidades dos cientistas, inclusive com a vertente póscustodial de Documentação, até que, em 1962 foi publicado um estudo, de autoria de Machlup, voltado a produção e distribuição de conhecimentos. Em 1963, um relatório de Weinberg apontou que as agências de governo fomentadoras de pesquisa científicas deveriam também assumir a responsabilidade pela transferência do conhecimento gerada nas pesquisas. (ARAÚJO, 2018).

Aqui tem-se a ponta de lança, na medida em que vários pesquisadores passam a estudar o processo da "comunicação da informação científica": o estudo dos vários registros do cientista, da ideia na sua cabeça (relatórios, seminários, apresentações em eventos, artigos em periódicos, livros, citações ao trabalho, menções em livros-textos e enciclopédia), até as suas características, vantagens e desvantagens, tempo médio de produção, entre outros aspectos, inclusive, amparar e buscar os dados, estejam estes em bibliotecas, em arquivos, em museus, em bases de dados, em artigos de periódicos, onde estiver, um estudioso da ciência da informação estará de "olhos abertos" e dedos disponíveis para cataloga-los. Qual seja, a "comunicação informal" passa a consolidar a concepção da Ciência da Informação e seu objeto de estudo - dos fluxos, dos caminhos percorridos pela informação, sua materialização em diferentes produtos e serviços – passa a ser uma importante lição e fundamentação à legislação, da qual a nova LPDP, é, sem dúvida, uma destacada resposta.

4 LEI DE PROTEÇÃO DE DADOS PESSOAIS: considerações e desafios

Devem ser destacados na LPDP alguns aspectos vinculados às tecnologias e que são por ela normatizados.

Estes pontos foram identificados como desafios tecnológicos a serem suplantados em razão da necessidade das novas exigências legais, de forma a se integrarem ou coexistirem com os sistemas de informação atuais e, neste aspecto, anunciar o estado da arte.

4.1 Anonimização (art. 11, § 3º, da Lei 13709/2018).

O processo de eliminação ou modificação da informação pessoal existente numa base de dados, com o objetivo de dificultar ou impedir a identificação unívoca dos indivíduos.

A referida lei dispõe sobre padrões e técnicas utilizados em processos de anonimização e regulamenta as possíveis verificações acerca de sua segurança. O grande desafio tecnológico

ainda é como utilizar os dados mesmo que anonimizados, por exemplo, no processo de busca de determinados dados sem comprometer a anonimização

De acordo com a utilização de técnicas e o alcance dos objetivos, podem ser considerados três divisões: de-identificação, anonimização e pseudonimização.

A de-identificação é o processo de remoção ou ofuscação de toda a informação pessoal de uma base de dados, com o objetivo de impedir a identificação dos indivíduos. É possível reverter a de-identificação através de uma tabela de mapeamento (ligando os registros originais aos registros de-identificados). Ela suprime todos os atributos identificadores e também modifica os "*quasi-identifiers"*, mediante processos de generalização.

Um nível mais elevado da de-identificação é a anonimização, quando a pretensão é tornar impraticável, ou até mesmo impossível (com o uso de todos os meios considerados razoáveis) a re-identificação. Este processo impossibilitaria inclusive o próprio técnico que realizou a operação inicialmente de reverter o procedimento. Merece destaque o fato da definição ser adaptável ao contexto tecnológico do momento: "*todos os meios considerados razoáveis*". A afirmativa leva à ponderação de quais seriam os recursos necessários, o custo do processo e o conhecimento necessário para realizar uma re-identificação.

Já a pseudonimização objetiva substituir todos os identificadores pessoais por palavras ou códigos gerados artificialmente, os quais poderão funcionar como representações mascaradas dos dados originais. Uma pseudonimização relevante possui uma preocupação adicional relacionada com a incidência sobre os atributos "*quasi-identifiers*" (por exemplo a data de nascimento), e que a atribuição de códigos seja realizada de forma aleatória e independente dos valores originais (muito embora podendo ocasionalmente continuar relacionados entre si).

Infelizmente, diversos casos têm evidenciado as falhas em processos de anonimização. Estas situações têm evidenciada a necessidade do envolvimento de especialistas nos processos de anonimização, já que qualquer erro poderá gerar repercussões na imagem da organização.

A simples remoção de atributos identificadores (nome, telefone, etc.) nunca será suficiente para eliminar os riscos de quebra de privacidade. Por outro lado, é constante a possibilidade de um *hacker* acessar outras bases de dados externas, possibilitando o cruzamento dessa informação com os dados que se pretendam anonimizar (Pinho, 2017).

4.2 Direito ao esquecimento (art. 16, Lei 13709/2018).

O direito ao esquecimento diz respeito aos direitos privativos da personalidade, corolário do direito à intimidade, à privacidade, à honra e à imagem, e, na sociedade da informação, apesar de conservar a pertinência com o princípio da dignidade do ser humano, diz respeito às inúmeras notícias disseminadas pelos meios de comunicação e tem vínculo com a proteção de dados, pessoais e sensíveis, de onde decorrem inúmeros problemas de violação da personalidade acarretada pela perpétua exposição de dados.

Nesse contexto, os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para algumas finalidades. Existem dificuldades técnicas para o seu cumprimento dada a grande quantidade de replicações e cópias de dados.

Os controladores são obrigados a fornecer relatórios de tratamento quando requisitados pelos titulares, sendo exigido não só uma plataforma de atendimento a essas requisições como também uma organização dessas informações internamente pelas instituições (art. 18).

Não só é necessário que a instituição consiga estruturar os dados requisitados de maneira que possa haver a portabilidade: ela deve prover os recursos técnicos e manter contato com outras instituições para que os canais de portabilidade funcionem corretamente (art. 18, inciso V).

4.3 Transferência internacional de dados (art. 33, Lei 13709/2018)

A transferência internacional de dados pessoais é permitida nos seguintes casos: a)para países ou organismos internacionais com grau de proteção de dados pessoais; b)quando o controlador apresentar garantias de cumprimento dos princípios, dos direitos e do regime de proteção de dados; c) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução; d)quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; e)quando a autoridade nacional autorizar a transferência e esta resultar em compromisso assumido em acordo de cooperação internacional; g)quando a transferência for necessária para a execução de política pública ou atribuição do serviço público; h)quando o titular tiver fornecido o seu consentimento específico para a transferência, com informação prévia sobre o caráter internacional da operação; i)quando necessário para atender as hipóteses seguintes: -para o cumprimento de obrigação legal ou regulatória pelo controlador; - para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; e -para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Cumpre também destacar que, nos termos da Lei nº 12527/2011, as pessoas jurídicas de direito público, na esfera de suas competências e atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção de dados pessoais dispensado pelo país ou organismo internacional.

No mesmo sentido da portabilidade, a transferência internacional de dados é um desafio para as instituições que necessitem/desejem efetuar a transferência não só pelos requisitos autorizados pela Lei quanto pelas dificuldades técnicas em efetuar essa empreitada.

4.4 Decisões automatizadas: (Art. 20, da Lei 13709/2018)

O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

A possibilidade de rever decisões automatizadas será um grande desafio para as instituições que trabalham com significativos volumes de dados – em qualidade e quantidade - pois seus sistemas terão que conter informações suficientes que justifiquem a decisão para que a mesma possa ser revista, se for o caso. Em larga escala, o atendimento a essas demandas também terá que ser incorporado aos

sistemas utilizados. Esse parece ser um desafio enorme para instituições que não tem a preocupação de segurança em tecnologia de *Big Data*.

4.5 Relatórios de impacto (Art. 38, Lei13709/2018)

A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referentes as operações de tratamento de dados, observados os segredos comercial e industrial das relações de negócios, e especialmente o sigilo e a confidencialidade entre pessoas e gestão.

As instituições deverão ter conhecimento e auditar seus sistemas para que os relatórios de impacto possam ser construídos, decorrentes de processos e procedimentos para o caso de vazamento de dados.

4.6 Boas práticas de segurança (Art. 46, Lei 13709/2018)

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado com vistas a impedir a configuração de ilicitudes.

Para tanto, as atividades de tratamento de dados pessoais, inclusive as relativas aos dados sensíveis, devem primar pela observância do princípio da boa-fé, bem como, caracterizada, sua finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação; responsabilização e prestação de contas, no caso, a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

É certo que pelo § 1º do art. 46 da LGPD, a autoridade nacional poderá dispor a respeito de padrões técnicos mínimos, visando tornar aplicáveis as disposições contidas no seu caput, para o qual levará em conta as seguintes situações: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente.

Embora ainda não estejam regulados pela autoridade, as instituições deverão atender a padrões técnicos para o tratamento de dados pessoais. Pela lei, entende-se que a autoridade irá apontar regularmente as revisões em virtude da evolução da tecnologia e de novos padrões de segurança (Apêndice D).

4.7 Privacidade por *default* e por *design*: (Art. 46, § 2º Lei)

As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Tanto na concepção dos sistemas que fazem tratamento de dados quanto na sua execução, deverão ser observadas as garantias, prerrogativas e diretrizes da lei para o tratamento de dados pessoais. Isso significa uma revisão completa dos sistemas que fazem esse tipo de tratamento, assim como uma preocupação para os sistemas que estão em desenvolvimento e que virão a ser desenvolvidos. Em sistemas mais antigos e integrados em diferentes plataformas, isso pode significar uma revisão completa ou até mesmo uma necessidade de reestruturação de sistemas inteiros, em virtude da complexidade de se ter um sistema com proteção de privacidade desta forma.

4.8 Vazamento de dados: Art. 48.

O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A construção dos relatórios de vazamento deverá ser pautada em informações acerca dos mesmos e nos riscos que eles representam, além das medidas que foram tomadas e serão tomadas acerca dos incidentes. Isso representa uma enorme mudança técnica no tratamento de dados pessoais das empresas, uma vez que a identificação de um vazamento, suas soluções técnicas imediatas e as mudanças que deverão decorrer em virtude dos mesmos representam um desafio tanto jurídico quanto tecnológico, pautando-se na segurança da informação.

5 RESULTADOS

Verifica-se que os objetivos propostos para o presente estudo foram atingidos uma vez que alguns dos principais problemas tecnológicos da lei foram elencados permitindo que se possa avançar, num futuro estudo, para a etapa dois, ou seja, para o "modelo de processo de resolução de problemas" (LAUDON; LAUDON, 2014, p. 20), pertinentes à implantação dos desafios tecnológicos nas organizações.

6 CONCLUSÃO

A identificação de alguns dos principais pontos dos desafios tecnológicos impostos pela Lei 13709/2018, permite a identificação de diferentes problemas que precisam ser resolvidos, e desta forma caracteriza a etapa 1 necessária para o "modelo processo de resolução de problemas" que poderá auxiliar as organizações a implantarem soluções adequadas e que satisfaçam as exigências legais de proteção de dados pessoais. Este primeiro passo é o ponto de partida para se criar um caminho rumo ao encontro das melhores soluções para a implantação da nova normatização de proteção de dados pessoais nas organizações.

REFERÊNCIAS

ARAÚJO, Carlos Alberto Ávila. **O que é Ciência da Informação?**. Disponível em http://www.uel.br/revistas/uel/index.php/informacao/article/view/15958/14205 Acesso em 15 nov 2018.

ASSOCIAÇÃO BRASILEIRA DE AGÊNCIAS DE PUBLICIDADE. **Cartilha Institucional de Segurança da Informação e Prevenção a Fraudes**. São Paulo. Disponível em < http://www.abap.com.br/pdfs/seguranca_informacao.pdf>. Acesso em 27/09/2018.

BRASIL. **Cilindro de Ciro**. Disponível em http://www.dhnet.org.br/direitos/anthist/marcos/cilindro/index.htm Acesso em 15 nov 2018.

BRASIL. **Lei n. 13709, de 14 de agosto de 2018**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 27/09/2018.

BRASIL. Descritores em Ciências da Saúde. Disponível em http://decs.bvs.br/cgi-bin/wxis1660.exe/decsserver/ acesso em 08/10/2018.

BRASIL. Tribunal de Contas da União. Cartilha de boas práticas em segurança da informação - 4ª Edição. Brasília. Disponível em <https://portal.tcu.gov.br/biblioteca-digital/cartilha-de-boas-praticas-em-seguranca-da-informacao-4-edicao.htm>. Acesso em 07/10/2018.

CAVOUKIAN, Ann; JONAS, Jeff. **Privacy by design in the age of big data**. Ontário. Disponível em: < https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf>. Acesso em 07/10/2018.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. Tradução de Daniel Vieira. São Paulo: Pearson, 2011.

HARBOUR, Pamela Jones. Privacy by design in law, policy and practice: a white paper for regulators, decision-makers and policy-makers. Ontário. Disponível em < http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf>. Acesso em 07/10/2018.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de Informação Gerenciais**. Tradução de Célia Taniwaki. São Paulo: Pearson Education do Brasil, 2014.

LOVELUCK, Benjamin. **Redes, liberdades e controle: uma genealogia política da internet**. Tradução de Guilherme João de Freitas Teixeira. Petrópolis: Vozes, 2018.

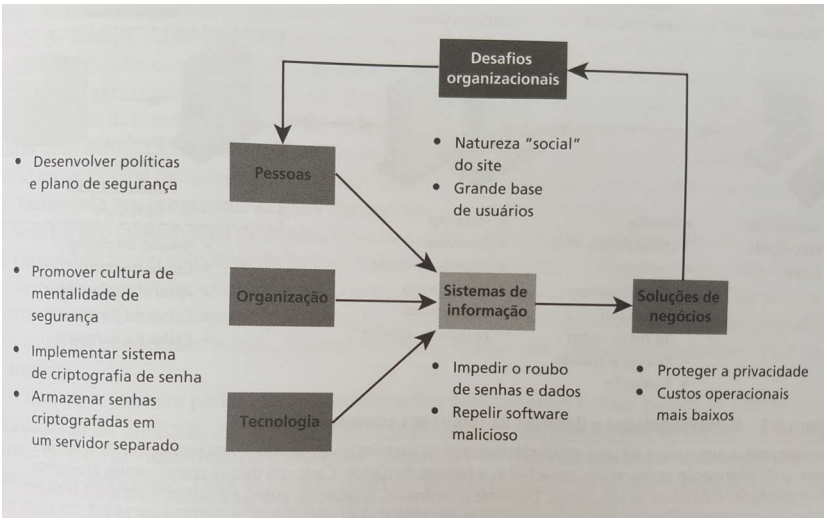
MARTINS, Claudia Aparecida et al. **Uma Experiência em Mineração de Textos Utilizando Clustering Probabilístico e Clustering Hierárquico.** São Carlos: Icmc, 2003.

PINHO, Frederico António Sá Oliveira. **Anonimização de bases de dados empresariais de acordo com a nova regulamentação europeia de proteção de dados**. Dissertação (Mestrado em Segurança Informática. Departamento de Ciência de Computadores. Faculdade de Ciências. Universidade do Porto. Porto, 2017.

PROVOST, Foster; FAWCETT, Tom. **Data Science para negócios**. Tradução de Marina Boscatto. Rio de Janeiro: Alta Books, 2016.

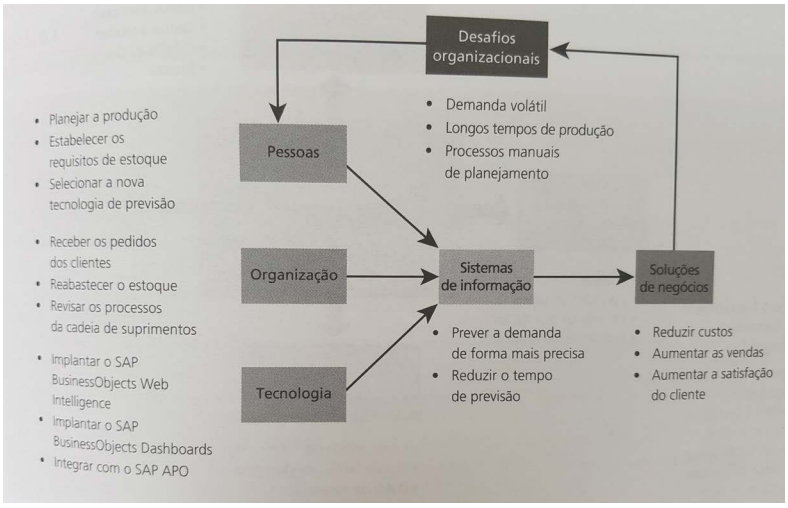
Sheshasaayee, Ananthi; Bhargavi. K. **A study of automated decision making systems**. Disponível em: < http://www.researchinventy.com/papers/v7i1/E07012831.pdf>. Acesso em 07/10/2018.
WIHLBORG, Elin; LARSSON, Hannu; HEDSTRÖM, Karin. "The Computer Says No!" - A Case Study on Automated Decision-Making in Public Authorities. Disponível em: <https://www.researchgate.net/publication/290303337_The_Computer_Says_No_--_A_Case_Study_on_Automated_Decision-Making_in_Public_Authorities>. Acesso em 07/10/2018.

Apêndice A –



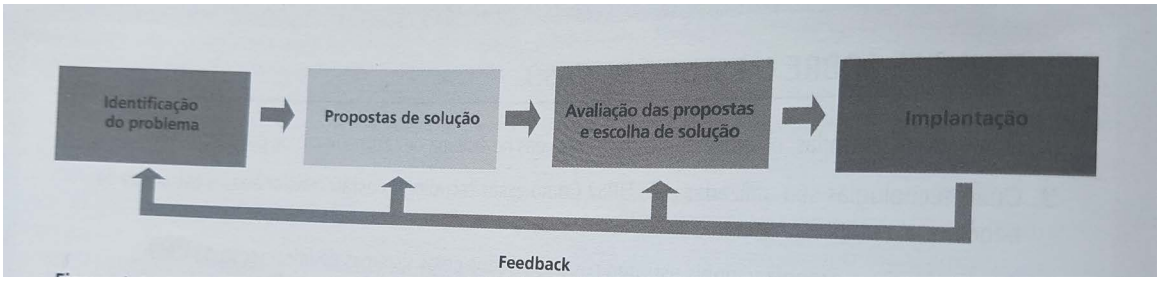
Sistemas de Informação Gerenciais, (LANDON; LANDON, 2014, p.255)

Apêndice B –



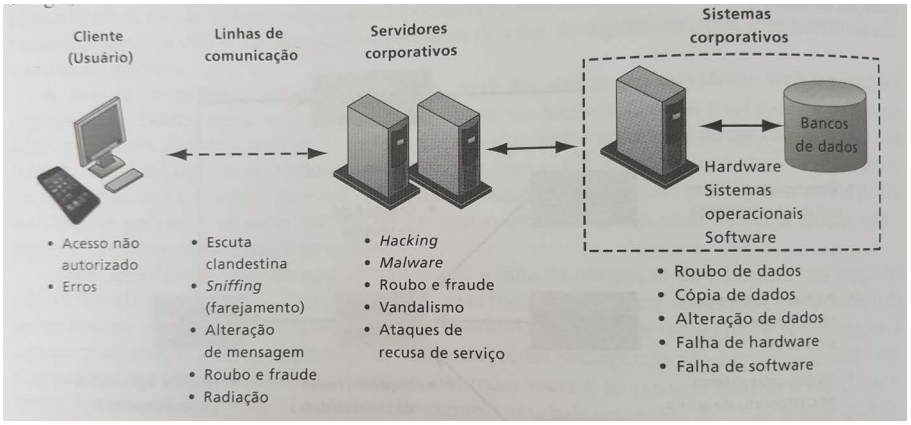
Sistemas de Informação Gerenciais, (LANDON; LANDON, 2014, p. 20)

Apêndice C –



Sistemas de Informação Gerenciais, (LANDON; LANDON, 2014, p. 20)

Apêndice D –



Sistemas de Informação Gerenciais (LANDON; LANDON, 2014, p. 256)