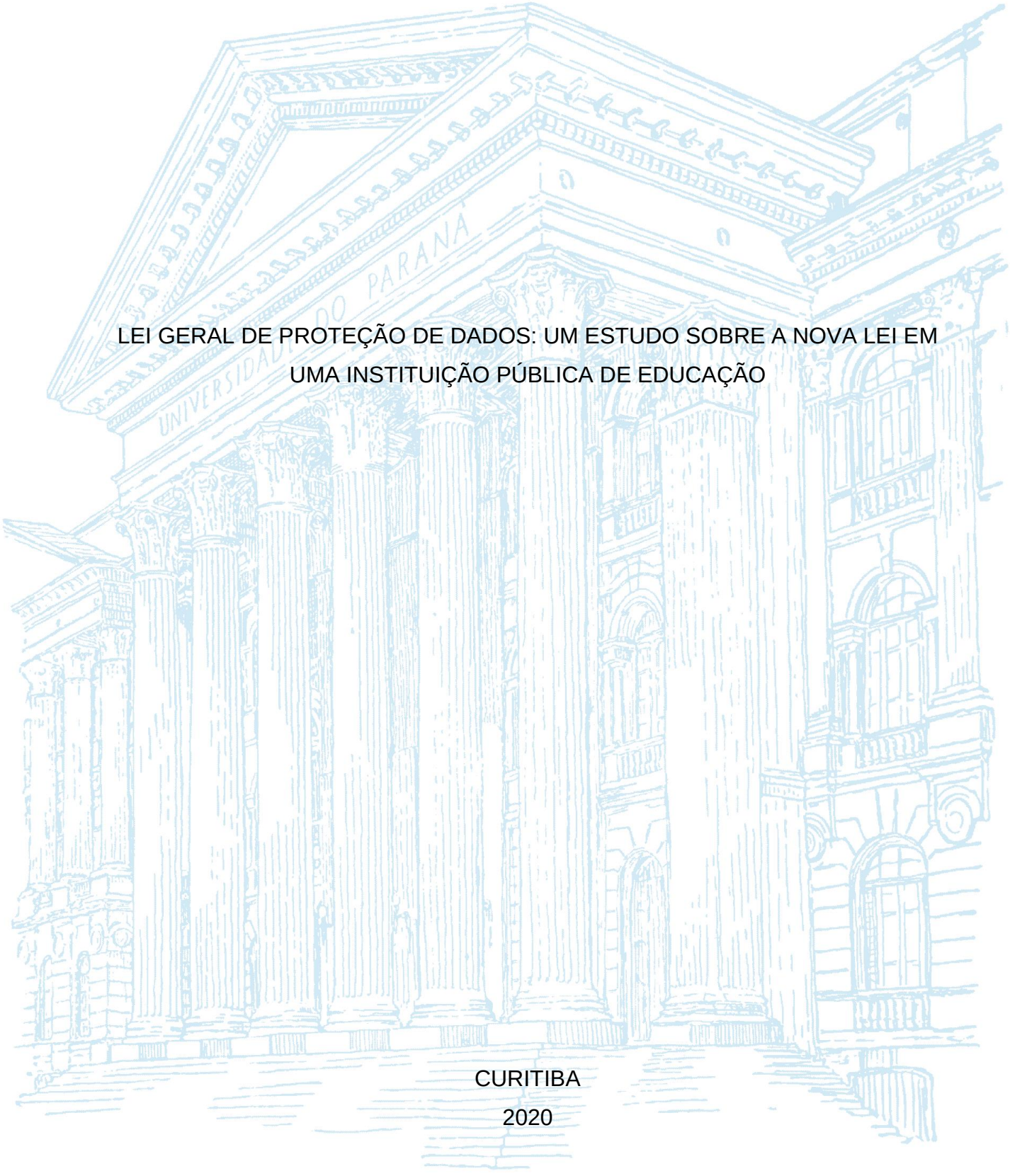
UNIVERSIDADE FEDERAL DO PARANÁ

FÁBIO CERVI DE MELLO



LEI GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO SOBRE A NOVA LEI EM UMA INSTITUIÇÃO PÚBLICA DE EDUCAÇÃO

CURITIBA

2020

Fábio Cervi de Mello

LEI GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO SOBRE A NOVA LEI EM UMA INSTITUIÇÃO PÚBLICA DE EDUCAÇÃO

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação, Setor de Ciências Exatas, Universidade Federal do Paraná, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

Orientadora: Profa. Ms. Elenice Mara Matos Novak

CURITIBA

2020

Aos meus pais, meus amigos e familiares, que sempre ajudaram e não deixaram desistir do meu sonho.

AGRADECIMENTOS

Primeiramente aos meus pais, que entenderam que esse era o curso que eu queria fazer e não tentaram mudar minha opinião. Por todas as vezes que não atingi as expectativas que tinham comigo, mas mesmo com todas as dificuldades continuaram a me apoiar.

À orientadora, Profa. Elenice Mara Matos Novak, pela caminhada durante o desenvolvimento desse trabalho. Por todas as nossas conversas, pelos convites para participar das aulas porque teria alguma palestra interessante, por todos os *links* e todas as informações compartilhadas para que esse trabalho pudesse ser escrito e pudesse ser aprovado.

Aos contatos feitos decorrente da escolha desse tema. Dos advogados a profissionais relacionados à nova Lei. Por terem tido a paciência com um aluno de graduação e terem disponibilizado um tempo em sua corrida rotina para escrever um e-mail ou ainda mais, por terem aceitado se encontrar comigo para conversarmos e tirarmos dúvidas que me ajudaram a compor este trabalho.

Aos meus amigos que continuam comigo desde os dias de ensino fundamental, de ensino médio, e na graduação cada um foi para o seu lado, mas estamos juntos e sempre me apoiaram. Alberto, Amanda, Daniel e todos os outros que estão comigo desde muito antes da UFPR, e tenho certeza que vamos continuar juntos. Amanda, obrigado pelos vários passeios, pelas conversas nos bancos e pelos trabalhos que ficávamos até o último dia fazendo para conseguir a maior nota possível, começamos juntos e terminamos juntos esse curso. Alberto, por mostrar que sim, a praia existe. Por aqueles dias incríveis em Penha na semana que saiu o resultado do vestibular, lá em 2015. Pelos nossos encontros na sua casa, onde ficávamos até de madrugada jogando e esquecíamos de tudo, só aproveitávamos. (Daniel) Dóris, primeiro, por sempre me responder onde ficava seu apartamento na praia. Por sempre estar ao meu lado, estarei sempre do seu também. Amanda, você que esteve do meu lado nesse ano de 2020, muito obrigado.

Muitos agradecimentos também vão para você Aline. Desde 2018 quando te procurei, você me ajudou e eu não estaria aqui hoje se não fosse nossas consultas semanais.

Sic Parvis Magna – Grandeza em Pequenos Começos

Sir Francis Drake

RESUMO

Este texto objetiva oferecer uma introdução sobre a nova Lei Geral de Proteção de Dados que entrou em vigor em 18 de setembro de 2020 e afetará diversos ramos das instituições públicas e privadas. Inúmeras instituições públicas e privadas que tratam de dados, e porventura armazenam e geram informações com esses dados de clientes, devem adequar-se para que fiquem em conformidade com a nova Lei e, consequentemente, não venham sofrer penalidades devido ao seu não cumprimento ou ao seu cumprimento parcial. Para que a adaptação ocorra são necessários profissionais que possuem conhecimentos técnicos, como analisar o sistema e verificar seu estado atual, implementar e implantar novos recursos e funcionalidades a um sistema de software já existente para que o mesmo fique em conformidade com a LGPD. Os profissionais também devem possuir orientação jurídica para saber se o sistema pelo qual ele é responsável está de acordo ou não com a Lei. Devido às penalidades desta nova Lei, as instituições públicas e privadas que não se adequarem à mesma podem sofrer consequências graves. Também são apresentadas duas metodologias utilizadas na Europa em função da GDPR para a privacidade dos dados. Foi realizado um estudo de caso na Universidade Federal do Paraná a partir das informações compartilhadas pela Agência de Tecnologia da Informação e Comunicação para saber o que já foi feito, o que está sendo e o que será realizado na Instituição de modo que a mesma fique de acordo com a LGPD.

Palavras-chave: Dados e Informações. Lei Geral de Proteção de Dados - LGPD. Profissional técnico e jurídico. Universidades.

ABSTRACT

This work aims to provide an introduction to the new General Data Protection Law (Lei Geral de Proteção de Dados - LGPD) that came into force on September 18, 2020 and will affect various branches of public and private institutions. Many public and private institutions that deal with data, and store and generate information from this data set, must adapt themselves so that they are in compliance with the new Law and, consequently, avoid penalties caused by non-compliance or partial compliance. For the adaptation to take place, professionals with technical knowledge are needed, people able to analyze the system and check its current state, and implementing new features and functionality to an existing software system so that it is in conformity with the LGPD. Professionals must also have legal guidance on whether the system for which they are responsible is in accordance with the Law or not. Due to the penalties of this new Law, public and private institutions that do not conform to it can suffer serious consequences. This text also presents two methodologies used in Europe according to the GDPR for data privacy. A case study was carried out at the Federal University of Paraná based on information shared by the Information and Communication Technology Agency to find out what has already been done, what is being done and what will be done at the Institution so that it remains in accordance with the LGPD.

Keywords: Data and Information. General Data Protection Law. Technical and Law professionals. Universities.

LISTA DE FIGURAS

FIGURA 1 – ESTRUTURA DA ISO 27001.....17

LISTA DE ABREVIATURAS OU SIGLAS

ANPD	- Autoridade Nacional de Proteção de Dados
CCE	- Centro de Computação Eletrônica
COPLAD	- Conselho de Planejamento e Administração
CPF	- Cadastro de Pessoa Física
DSInf	- Departamento de Segurança da Informação
LGPD	- Lei Geral de Proteção de Dados
MEC	- Ministério da Educação
PDTIC	- Plano Diretor de Tecnologia de Informação e Comunicação
PROGRAD	- Pró-Reitoria de Graduação
PRPPG	- Pró-Reitoria de Pesquisa e Pós-graduação
PSI/UFPR	- Política de Segurança da Informação na Universidade Federal do Paraná
RIPD	- Relatório de Impacto de proteção de dados
SGSI	- Sistema de Gestão de Segurança de Informação
T.I.	- Tecnologia da Informação
TIC	- Tecnologia da Informação e Comunicação
UFPR	- Universidade Federal do Paraná
DPO	- *Data Protection Officer*
FAQ	- *Frequently Asked Questions*
GDPR	- *General Data Protection Regulation*
OWASP	- *Open Web Application Security Project*
NIST	- *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*

SUMÁRIO

1 INTRODUÇÃO 11

1.1 OBJETIVO 11

1.1.1 Objetivo geral 12

1.1.2 Objetivo específico 12

2 JUSTIFICATIVA 12

3 EMBASAMENTO TEÓRICO 13

3.1 OCORRÊNCIAS 15

3.2 ISO 27001 E OUTRAS PRÁTICAS DE PROTEÇÃO DE DADOS 16

3.3 LGPD 19

3.3.1 Dados pessoais, dados sensíveis e dados anonimizados 30

3.3.2 DPO 31

3.4 *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT* 34

3.5 MANUTENÇÃO 35

4 ESTUDO SOBRE A LGPD EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR: UNIVERSIDADE FEDERAL DO PARANÁ 39

4.1 AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (AGTIC) 39

4.2 RESOLUÇÃO N° 21/14-COPLAD 41

4.3 LGPD EM 2020 NA UFPR 48

5 CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS 60

5.1 CONCLUSÕES 60

5.2 RECOMENDAÇÕES PARA TRABALHOS FUTUROS 67

REFERÊNCIAS 68

1 INTRODUÇÃO

A partir de 18 de setembro de 2020, a nova Lei Geral de Proteção de Dados - LGPD (Lei N° 13.709/2018) entrou em vigor. Baseando-se na legislação europeia já existente, a *General Data Protection Regulation* (GDPR), a LGPD foi criada com base no direito à privacidade dos dados, no direito à liberdade e visando ao desenvolvimento tecnológico do país.

A Lei N° 13.709/2018 e seus 65 artigos são apresentados nesse trabalho de forma que possam explicar as novas figuras decorrentes da LGPD, a Autoridade Nacional de Proteção de Dados, as punições que podem vir a ocorrer e como estão sendo aplicadas as normas presentes através de ações em uma Universidade Pública.

Devido à abrangência da LGPD, este trabalho foca em sua aplicação em uma Instituição de Ensino Superior, a Universidade Federal do Paraná (UFPR). Para isso, foram realizadas reuniões com a Agência de Tecnologia da Informação e Comunicação (AGTIC) da Universidade, nas quais houve o compartilhamento de informações sobre quais práticas estavam sendo realizadas e quais ações ainda serão executadas para que a Instituição fique completamente de acordo com as novas regras.

1.1 OBJETIVO

O objetivo desse trabalho é fazer uma análise de um ambiente de T.I. em uma Universidade Pública e demonstrar as devidas modificações que devem ser feitas para que a instituição fique de acordo com a nova Lei Geral de Proteção de Dados. Foi escolhida a UFPR como objeto de estudo e, dentro da Instituição, foram verificados quais princípios da Lei já foram abordados e de qual forma, quais os planos que existem para que a Universidade fique completamente de acordo com as novas regras e quais são as ações que já ocorreram para entrar em concordância com a Lei.

1.1.1 Objetivo geral

A partir de pesquisas e de contato com uma Instituição de Ensino Superior (IES) desenvolver um documento contendo informações sobre ações e planos da Universidade para que fique em concordância com a Lei Geral de Proteção de Dados.

1.1.2 Objetivo específico

Verificar quais são as políticas e ações que a Universidade Federal do Paraná em seus órgãos internos competentes realizou, está realizando e realizará para que Instituição fique de acordo com a LGPD.

2 JUSTIFICATIVA

De acordo com o que foi escrito por Henrique Somadossi em seu artigo publicado no site Migalhas “O cotidiano das empresas está prestes a sofrer novo marco regulatório que as impactará como poucas leis antes fizeram.” [12]. A criação da LGPD foi motivada pelos diversos escândalos envolvendo dados que afetaram milhares de usuários, de acordo com Vinicius Durbano em artigo publicado no dia 26 de setembro de 2019 no site de segurança digital Ecoit [13], e também pelo Brasil não possuir uma legislação ampla com relação a este assunto.

Em 2016 na União Europeia, a *General Data Protection Regulation* (GDPR) foi aprovada. A GDPR foi idealizada em 2012 e 4 anos depois aprovada; embora a região já possuísse leis relacionadas a privacidade, estas encontravam-se defasadas por serem de 1995, um cenário bem diferente do vivido atualmente. Existem diversos pontos sobre os quais a Lei da União Europeia trata, tais como:

- O serviço que utilizará os dados do usuário deve permitir que o mesmo escolha como seus dados serão usados, e estes somente serão utilizados se o usuário consentir;
- O usuário tem o direito de saber como e quais dados seus estão sendo utilizados e para quais finalidades;

- A linguagem utilizada nos sistemas deve ser clara para que o usuário leigo seja capaz de entender o que acontecerá com seus dados;
- Quando um novo sistema for implementado, a proteção dos dados deve ser pensada desde o início do projeto, constituindo parte essencial do mesmo.

De acordo com o Código de Defesa do Consumidor e com a Lei do Cadastro Positivo, o direito à explicação e a revisão de decisões automatizadas são garantidos ao consumidor no âmbito das relações de consumo. A LGPD foi criada para utilização em qualquer contexto, setor ou mercado que processem dados, e esses dois direitos podem ser efetivamente utilizados por qualquer pessoa que necessite.

Diversos princípios são aplicados à Lei Geral de Proteção de Dados. Por exemplo, a Lei garante que o titular dos dados tem direito à transparência de seus dados, ou seja, ele pode obter informações claras e precisas sobre o processo ao qual seus dados são submetidos. Também é garantido que o proprietário dos dados (usuário) tenha conhecimento sobre os tratadores de dados, aqueles que tratarão (farão o uso) seus dados na instituição pública ou privada.

Serão apresentados agora alguns dos problemas que podem afetar as instituições públicas e privadas, como problemas de implementação (o que deve ser feito e como deve ser feito para ficar de acordo com a nova legislação) decorrentes do não cumprimento da Lei. Através de pesquisas e reuniões com pessoas do meio jurídico e de pessoas que convivem na AGTIC da Universidade Federal do Paraná foram elencados os temas aqui apresentados e, com base nesses estudos, são discutidas as medidas que devem ser tomadas, e como devem ser tomadas, na aplicação de diretrizes para que uma Universidade Pública fique de acordo com a Lei.

3 EMBASAMENTO TEÓRICO

Este capítulo apresenta a pesquisa realizada no decorrer do desenvolvimento do presente trabalho.

Parte-se do princípio que a Lei está em vigor, porém ainda não é aplicado nenhum tipo de multa. Somente a partir de agosto de 2021 será permitida a

aplicação de punições decorrentes do não cumprimento das novas regras impostas pela LGPD, assinada pelo Presidente em junho através da Lei N°14.010/2020 [29].

Porém, conforme pesquisa feita com mais de 400 instituições privadas – realizada entre junho e julho de 2020 e publicada pela Revista Exame – é mostrado que 64% das instituições privadas não estão em conformidade com a LGPD. Desse percentual, 24% das entrevistadas já estão em processo de adaptação; aquelas que têm conhecimento da Lei mas ainda não iniciaram suas mudanças somam 16%, e as que não sabem do que a LGPD trata são 24% das entrevistadas [15].

Os resultados de outra pesquisa, dessa vez realizada pela Serasa Experian, mostram que 72% das companhias que possuem mais de 100 funcionários pretendem contratar alguém especializado, externo à instituição, para que esta pessoa preste consultoria de forma que a empresa possa se adequar à nova Lei [14].

Essas alterações são relacionadas com as novas diretrizes sob as quais os dados devem ser submetidos. Todas as instituições públicas e privadas que obtêm dados de alguma forma de seus clientes ou usuários estão sujeitas às penalidades previstas em Lei e, como as consequências podem ser muito graves, é possível que a não conformidade com a Lei leve a instituição privada a possíveis colapsos devido ao valor da multa [2].

Para garantir que a Lei seja cumprida foi criada (em nove de julho de 2019) a Autoridade Nacional de Proteção de Dados (ANPD), a qual fica responsável por editar as regras e fiscalizar os procedimentos sobre a proteção de dados pessoais. A Agência será a responsável por aplicar punições aos que não estiverem de acordo com a Lei e deve arquitetar as regras e normas que dizem respeito aos dados pessoais dos brasileiros. Logo, diversas instituições públicas e privadas que não estiverem adequadas à LGPD poderão estar ameaçadas e sujeitas a penalidades e sanções por parte da ANPD, que podem ocorrer na forma de multas ou até mesmo na inviabilização do modelo de negócios adotado pela instituição [43] [44].

Hoje existem várias instituições públicas e privadas que já estão de acordo com a Lei. Aquelas que ainda não estão procuram adequar seu sistema, para que fique pronto o mais rápido possível e antes da ANPD começar a punir as que não estão em conformidade com as novas regras. Com a Lei em vigor, a conformidade com a mesma se torna um requisito adicional no momento em que uma instituição privada é escolhida para a prestação de um serviço. Se a instituição a ser contratada já

possui atualização em seu sistema para ficar em concordância com a LGPD, se já está sabendo da Lei e está em processo de modernização de seu sistema, essa instituição adquire uma vantagem competitiva em relação às suas concorrentes caso estas não possuam as regras implementadas, não estejam em processo de desenvolvimento das mudanças necessárias ou desconheçam a Lei atualmente [1].

Em seguida, serão apresentados alguns casos de instituições privadas e públicas que sofreram vazamento de dados nos últimos anos e comprometeram seus usuários.

3.1 OCORRÊNCIAS

A LGPD vem para tentar evitar que casos como os que ocorreram com grandes instituições públicas e privadas internacionais (Facebook®, Newegg e Aadhaar, por exemplo) venham a acontecer no Brasil. O caso do Facebook ficou conhecido mundialmente quando a empresa Cambridge Analytica utilizou dados e informações de usuários da rede social para que, dependendo da análise feita a partir dos dados, uma propaganda mais convincente pudesse ser exibida para o utilizador na época da eleição presidencial dos Estados Unidos, em 2016. Já em relação à loja Newegg, foi um caso no qual hackers obtiveram dados dos clientes toda vez que uma compra era concretizada. De 14 de agosto a 18 de setembro de 2018, todas as compras feitas na loja tinham as informações do cartão de crédito utilizado enviadas para um servidor controlado pelo grupo hacker [45].

Já o incidente da Aadhaar, uma agência governamental da Índia, permitiu que os dados de mais de 1 bilhão de pessoas pudessem ser acessados por qualquer um que pagasse a taxa que o grupo hacker pedia [46].

Como pode ser observado, grandes sistemas de grandes instituições públicas e privadas estão sujeitos a ataques, e os usuários são os mais afetados.

A seguir, haverá uma descrição a respeito da Norma ISO 27001, a qual trata de um padrão para a gestão de segurança da informação. Além disso, também serão citadas outras normas relativas à proteção de dados.

3.2 ISO 27001 E OUTRAS PRÁTICAS DE PROTEÇÃO DE DADOS

A ISO 27001 descreve como gerenciar a segurança de informação de uma organização, seja ela pública ou privada, com ou sem fins lucrativos, grande ou pequena. Sua versão mais recente é a 2013, sua primeira versão foi a 2005, e é uma norma estruturada com base na Norma Britânica BS 7799-2. Essa ISO determina estruturas para a elaboração de métodos para o gerenciamento dos dados dentro de uma instituição [31].

Conforme escrito por Longinus Timochenco, autor do artigo “Como a ISO 27001 pode ajudar a sua empresa com a LGPD” publicado no site Infra News Telecom, a LGPD exige das instituições medidas para a proteção de dados, e a ISO 27001 também requer medidas similares para que os riscos de violações sejam minimizados. Dessa forma, estar em conformidade com a ISO 27001 demonstra uma atitude semelhante de aproximação sucessiva à nova Lei [3].

Confidencialidade, integridade e disponibilidade dos dados, estas são as principais preocupações abordadas pela norma, não importando tamanho, função e tipo de instituição (pública ou privada) [16]. Para que isso ocorra, duas ações principais devem ser tomadas:

- Primeira fase – Avaliação de Risco: é formada pela análise dos dados e identificação de possíveis riscos relacionados aos mesmos;
- Segunda fase – Tratamento/Mitigação de Risco: é formada pela definição dos passos a serem tomados para que os problemas elencados na fase de Avaliação de Risco não venham a acontecer.

A Figura 1 apresenta a estrutura básica da norma.

FIGURA 1 – ESTRUTURA DA ISO 27001

Fonte: https://advisera.com/wp-content/uploads/sites/5/2014/05/frameworkPT.jpg

A implementação da Norma pode ajudar várias instituições que já possuem todo o seu software e hardware instalado e sendo executado, porém de forma não totalmente segura. A ISO não diz respeito apenas à implementação em software e/ou hardware, mas também interfere na gestão de negócios, políticas da organização e pessoas [16].

Além disso, a Norma possui referências sobre como tratar informações não digitais, tais como papéis ou documentos escritos à mão. Uma vez que esses passos tenham sido implementados, testados e aprovados, considera-se que o Sistema de Gestão de Segurança da Informação (SGSI) foi concluído com sucesso.

Junto com a ISO 27001 existem alguns benefícios que podem ser atingidos com a implementação desta norma de segurança da informação [16] [17] [18]. Essas vantagens são:

- Possuir a certificação é entendido pela LGPD como boa prática na tentativa de prevenção ao incidente de dados, podendo, em caso comprovado pela Autoridade Nacional de Proteção de Dados, haver atenuação de multa [52].

- Obtenção de vantagem em relação aos concorrentes: a instituição com a certificação terá preferência em relação àquelas que não apresentam a ISO 27001;
- Redução de custos: como um dos focos da ISO 27001 é a prevenção de riscos, a probabilidade de haver perda financeira é pequena.

Porém, conforme escrito por Vitor de Andrade e Stella Kim em seu artigo intitulado “Possuir a certificação ISO/IEC 27001:2013 significa estar Compliance com a LGPD? E quais as expectativas para a ISO/IEC 27701:2019?” para o site Migalhas, “[...] somente as boas práticas também não garantem a efetiva implementação da LGPD”. Além disso, de acordo com Andrade e Kim existia uma lacuna normativa no âmbito organizacional envolvendo segurança de dados, e para cujo preenchimento foi desenvolvida a ISO 27701, a qual veio complementar os aspectos da privacidade e proteção de dados [52].

A Norma ISO 27701 trata-se de um Sistema de Gestão de Segurança Privada que é uma extensão da ISO 27001, que tem por objetivo incluir novas ferramentas para garantir a total privacidade dos dados pessoais [53].

Juntamente com as ISO 27001 e 27701 apresentadas existem também outras práticas de segurança da informação como a OWASP (*Open Web Application Security Project*), uma comunidade que cria ferramentas, artigos, documentação, metodologias e tecnologias relacionados à segurança de aplicações online. [54]

Existe também o NIST (*National Institute of Standards and Technology*) que, de acordo com o site TI Inside, é um “[...] conjunto útil de estratégias de proteção de privacidade para organizações que desejam melhorar sua abordagem ao uso e proteção de dados pessoais”. Conforme a publicação, o NIST ajuda na identificação de necessidades e o que deve ser priorizado para satisfazê-las [55].

A seguir, será apresentada a Lei Geral de Proteção de Dados Pessoais assim como a classificação na qual os dados podem ser inseridos e o papel do Encarregado de Proteção de Dados.

3.3 LGPD

A LGPD foi aprovada pouco tempo depois de a União Europeia publicar, em 25 de maio de 2018, o seu Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation* - GDPR) [4].

Através da LGPD, o Brasil passa a compor um grupo de mais de 100 países, os quais possuem um regulamento adequado que rege os dados e as informações dos usuários, juntamente com a sua privacidade, de acordo com o site Agência Brasil [47].

No artigo intitulado “LGPD exigirá esforço multidisciplinar” para o site Security Report, Eduardo Batista, sócio de Cyber Security & Privacy da PWC, diz que “[...] esse esforço deve ser multidisciplinar e envolver áreas distintas, e não apenas as áreas de Segurança e Tecnologia.” Batista também destaca que a LGPD é multidisciplinar, pois exige sinergia de competências entre as áreas jurídica, tecnológica e processual para que ocorra a criação efetiva de um programa de segurança [50].

Conforme Paulo Oliveira – especialista em privacidade e segurança da informação – cita em artigo publicado no site Infra TI “Não adianta gastar recursos, infraestrutura e ferramentas, se a questão humana não estiver ciente do valor estratégico do dado” [56].

Um dos principais tópicos que é tratado na Lei diz respeito à transparência dos dados, ou seja, o titular dos dados deve saber exatamente onde seus dados serão utilizados, como serão utilizados, por que foram solicitados e por quem foram ou serão utilizados. Recomenda-se também que a coleta de dados seja restrita ao mínimo necessário, e que todos os dados coletados sejam excluídos após terem sido utilizados [2].

As operações que a Lei engloba são várias: formas de coleta de dados, mecanismos e maneiras de utilização, acesso, compartilhamento, processamento e armazenamento. Seja qual for a operação que envolva dado pessoal – este sendo definido como qualquer informação relacionada a uma pessoa natural identificada ou identificável – de acordo com o item 1 do artigo 5 da Lei, coletado de pessoa física ou jurídica em território brasileiro, seja em instituição pública ou privada, deve estar de acordo com a LGPD. A Lei N° 13.709/2018 define que o titular forneça consentimento para que o tratamento dos dados pessoais e sensíveis seja realizado,

porém, conforme os artigos 7 e 11 da Lei N° 13.709, existem situações nas quais o tratamento é permitido sem esse consentimento explícito do titular [2].

Com relação ao tratamento, está descrito no item 10 do artigo 5 que a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração são todas formas de tratamento de dados.

Ao todo a Lei N° 13.709/2018 possui 65 artigos. O artigo 2 discorre a respeito dos fundamentos da proteção de dados pessoais, os quais são:

I. O respeito à privacidade;
II. A autodeterminação informativa;
III. A liberdade de expressão;
IV. A inviolabilidade da honra e da imagem;
V. O desenvolvimento tecnológico, econômico e inovação;
VI. A defesa do consumidor e a livre concorrência;
VII. Os direitos humanos, dignidade e a prática da cidadania.

Em relação ao terceiro artigo, este trata sobre as operações realizadas com os dados, desde que o tratamento dos mesmos seja realizado no Brasil ou cujo objetivo é a oferta ou fornecimento de serviços ou bens, ou os dados sejam de pessoas localizadas em território nacional. Neste mesmo artigo, no item 3, é definido que também estão sujeitos às regras de tratamento de dados pessoais, não importando a localização onde serão feitas as operações e/ou armazenamento, dados que tenham sido coletados no Brasil.

Não estão cobertos pela LGPD operações de tratamento de dados cujas finalidades sejam pessoais sem envolvimento econômico, jornalísticas, acadêmicas, defesa nacional e segurança pública, conforme previsto no Artigo 4, itens 1, 2 e 3. Já no item 4, é estabelecido que dados vindos de fora do país, desde que no local de origem exista uma legislação de proteção de dados, também estão fora do escopo da LGPD.

Juntamente com a nova Lei, novas figuras surgirão no meio das instituições públicas e privadas, estas são o Controlador e o Operador. Ambas podem ser uma pessoa física ou jurídica, e em caso de pessoa jurídica, pode ser tanto pública

quanto privada. As tarefas do controlador são referentes às decisões sobre o tratamento dos dados coletados, enquanto as do operador são funções relacionadas ao tratamento dos dados baseados nas escolhas do primeiro, como descrito no artigo 5 nos itens 6 e 7 [2]. Há também uma terceira figura – que configura simultaneamente a criação de um novo cargo – a do Encarregado de Proteção de Dados (também conhecido com DPO – *Data Protection Officer*), que é indicado pelo controlador e pelo operador, e é responsável pela comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), conforme descrito no item 8 do mesmo artigo prévio [2].

Para o tratamento dos dados, deve-se observar as seguintes concepções, de acordo com o artigo 6 da Lei [2]:

I. Finalidade: todo tratamento deve ser informado ao titular e seu intuito seja lícito;
II. Adequação: compatível com finalidades informadas ao titular;
III. Necessidade: utilizar somente os dados necessários, conforme descrito no informe ao titular;
IV. Livre acesso: os titulares devem ter acesso fácil à forma, à duração do tratamento e à integridade de seus dados;
V. Qualidade dos dados: para que seja cumprido o objetivo do tratamento os dados devem ser exatos, claros e relevantes;
VI. Transparência: informações claras, precisas e com acesso fácil devem ser disponibilizados aos titulares;
VII. Segurança: garantir a segurança dos dados através de técnicas para sua proteção e evitar danos;
VIII. Prevenção: adoção de métodos para prevenir danos aos dados;
IX. Não discriminação: deve-se somente realizar um tratamento de dados caso sua finalidade seja permitida por lei;
X. Responsabilização: deve ser mostrada a adoção de ações que corroborem o cumprimento das medidas de proteção e sua eficácia.

O uso compartilhado de dados pessoais pelo Poder Público deve atender às finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitando os princípios de proteção de dados

pessoais presentes no artigo 6 da LGPD, como, por exemplo, a finalidade, adequação, necessidade e segurança.

Conforme também presente no texto da Lei, é vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

- Nos casos em que os dados forem acessíveis publicamente;
- Na hipótese de a transferência dos dados objetivar exclusivamente à prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidade [10].

Um tratamento de dados pessoais pode ser executado sem haver o consentimento explícito do titular, de acordo com os incisos II a X do artigo 7, os quais explicam em que situação é permitida a operação sem a autorização explícita. Para o cumprimento de leis pelo controlador ou pela administração pública para a aplicação de políticas previstas em leis, isso conforme os itens 2 e 3 do artigo 7 da LGPD [2]. Em caso de estudo realizado por órgão de pesquisa deve ser feita, sempre que possível, a anonimização dos dados, de acordo com artigo 7, item 4. Também é permitido o tratamento de um dado pessoal para a proteção da integridade do titular ou de um terceiro, assim como para a manutenção da saúde, nesse caso exclusivamente de profissionais de saúde, de acordo com os itens 6 e 7, respectivamente, desse mesmo artigo da Lei N° 13.709 [2].

O consentimento, ao qual se refere o item 1 do artigo 7 previamente mencionado, deve ser fornecido por escrito ou de alguma outra forma que mostre o consentimento do titular a respeito do que será feito com seus dados, conforme consta no artigo 8. Esse consentimento pode ser revogado a qualquer momento caso essa seja a decisão do titular, como está escrito no parágrafo 5 do artigo prévio [2].

O artigo 9 da LGPD remete a todos os itens que devem estar presentes e de forma clara a respeito do tratamento dos dados [2]. Dentre as informações pode-se citar a finalidade, a forma como será conduzido, o tempo que vai durar, a identificação de quem é o controlador e as informações sobre ele.

O tratamento de dados sensíveis poderá ser realizado quando o titular consentir de forma explícita que seus dados sejam utilizados de acordo com o inciso I do artigo 11. Porém, nas determinadas situações presentes no inciso II do mesmo artigo da Lei N° 13.709/2018 não é necessário esse consentimento explícito. Caso exista necessidade do cumprimento de leis, proteção da vida ou da saúde, também é permitido o tratamento, em conformidade com o artigo 11 da Lei [2].

Com relação aos dados de crianças e adolescentes, o tratamento desses somente poderá ser realizado mediante consentimento por pelo menos um dos pais ou responsáveis. Somente poderá ser coletado dado pessoal sem consentimento caso seja necessário o contato dos pais, sem armazenamento e utilizado somente naquela ocasião, conforme descrito no artigo 14, presente na seção III da LGPD [2].

Os artigos 15 e 16, constantes da seção IV do texto da Lei, discorrem sobre o fim do tratamento dos dados, que ocorre quando a finalidade é atingida, o período do tratamento é chegado ao fim, o titular decide que não quer mais participar ou é terminado pela Autoridade Nacional [2]. Da mesma forma, os dados pessoais devem ser eliminados após fim do tratamento, salvo algumas exceções como o cumprimento de alguma obrigação legal ou o estudo por órgão de pesquisa. Porém, sempre que possível deve ser realizada a anonimização dos dados pessoais utilizados.

Em se tratando de direitos do titular, o artigo 17 da Lei N° 13.709 – que faz parte do Capítulo III da Lei, cujo título é “Dos Direitos do Titular” – diz que toda pessoa tem a titularidade de seus dados pessoais e seus direitos fundamentais assegurados [2].

A partir do controlador, o titular pode coletar informações sobre o tratamento dos dados, o acesso a eles e corrigir ou adicionar informações faltantes. É possível também descobrir com quais instituições públicas e/ou privadas o controlador compartilhou seus dados e a eliminação de seus dados, bastando para tal apenas uma requisição, conforme descrito no artigo 18 [2].

Sobre a requisição, a mesma pode ter desde um formato mais simples até a apresentação de declaração completa, contendo todos os dados relevantes (finalidade do tratamento, origem dos dados). O retorno das informações para o titular pode ser tanto realizado por meio digital como impresso. Essas informações estão presentes no artigo 19 da LGPD [2].

Caso o titular não concorde com alguma decisão automatizada tomada com base em seus dados ele tem o direito de solicitar a revisão dessa escolha, de acordo com o artigo 20 da Lei Geral de Proteção de Dados. Caso seja feita essa solicitação de revisão, o controlador deve fornecer todas as informações que foram levadas em conta no momento da análise e, como esse resultado foi atingido, conforme o parágrafo 1 artigo citado previamente. Já o artigo 21 da Lei define que um dado não pode ser utilizado de forma prejudicial a seu titular [2].

O capítulo IV da LGPD aborda o tratamento dos dados pessoais pelo poder público, e seu primeiro artigo, 23, discorre justamente sobre isso. As pessoas jurídicas que realizarem operações com dados pessoais devem somente realizar tais operações com finalidade de interesse público [2].

Todos os dados devem ser mantidos em formato interoperável para uso compartilhado cujo intuito seja a execução de políticas públicas, prestação de serviços públicos, entre outros, conforme o artigo 25 da Lei N° 13.709 [2].

Com relação ao compartilhamento de dados para uso pelo poder público, o artigo 26 descreve que somente pode ser feito caso o objetivo seja a execução de políticas públicas [2].

A ANPD poderá, a qualquer momento, determinar novas regras para a comunicação e o uso compartilhados de dados pessoais, conforme artigo 30 da LGPD [2] [5].

Caso um órgão público realize alguma atividade que seja considerada em desacordo com a Lei Geral de Proteção de Dados, a Autoridade Nacional pode enviar um documento contendo medidas que considere adequadas para que não ocorra novamente tal problema, de acordo com o artigo 32, seção II, do texto da LGPD [2].

O capítulo V da Lei trata sobre a transferência internacional de dados, englobando do artigo 33 ao 36. Somente é permitida a transferência internacional de dados pessoais para outros países que possuam uma legislação com algum nível de proteção de dados condizente com a LGPD, conforme definido no item 1 do artigo 33. A ANPD pode avaliar características referentes aos dados que estão sendo enviados para outro país assim como as Leis presentes no destino dos dados, como, por exemplo, o tipo dos dados que estão sendo transferidos, a adoção de medidas de segurança previamente estabelecidas, entre outros, de acordo com os itens 2 e 4, respectivamente, do artigo 34 [2].

Qualquer alteração que venha a ocorrer em relação às garantias que uma vez foram consideradas suficientes em relação à proteção de dados e/ou referente aos direitos do titular devem ser comunicadas à Autoridade Nacional, vide artigo 36 [2].

Referente aos agentes de tratamento de dados, o capítulo VI, seção I, discorre sobre o controlador e o operador. Seu primeiro artigo, 37, diz que tanto o operador como o controlador devem manter registro sobre as operações de tratamento de dados que executarem. A ANPD pode pedir ao controlador a elaboração de um documento que relate o impacto à proteção dos dados pessoais, adicionando os dados sensíveis, relativo às operações de tratamento de dados executadas, como é dito no artigo 38. As tarefas cujas responsabilidades são do operador serão definidas pelo controlador, conforme o artigo seguinte cita. Já o último artigo desta seção, 40, informa a possibilidade de a Autoridade Nacional fornecer padrões para que a portabilidade e o livre acesso aos dados ocorram, considerando sua necessidade e transparência [2].

A seção II do capítulo VI comenta sobre o encarregado pelo tratamento dos dados pessoais, sendo que em seu primeiro artigo, 41, é escrito que “O controlador deverá indicar encarregado pelo tratamento de dados pessoais”. Conforme o primeiro parágrafo desse artigo, uma vez que seja escolhido o encarregado, suas informações de contato devem ser divulgadas publicamente. No parágrafo seguinte são citadas algumas de suas responsabilidades, que incluem:

I. Aceitar reclamações dos titulares;
II. Receber comunicação da autoridade nacional;
III. Executar atividades determinadas pelo controlador.

A seção III deste capítulo, cujo título é “Da Responsabilidade e do Ressarcimento de Danos”, possui 4 artigos, sendo que o primeiro, 42, informa que é de obrigação do controlador ou do operador que, caso algum desses infrinja qualquer dano através das operações utilizando dados pessoais, seja reparado e o titular indenizado. Somente não serão culpados o operador e/ou controlador caso seja provado que não foram eles os responsáveis pelo dano; que, mesmo com o tratamento realizado com os dados, não houve violação à legislação; ou que o dano é de culpa interinamente do titular, vide artigo 43 da Lei N° 13.709/2018. Caso as operações sobre as quais os dados serão submetidos não ofereçam proteção

adequada ou não respeitem a legislação, será considerada irregular, de acordo com o artigo 44 [2].

No capítulo VII, a seção I se refere à segurança e à confidencialidade dos dados, e o artigo 46 cita que os agentes responsáveis pelo tratamento dos dados são obrigados a adotar medidas de segurança, elencando campos administrativos e técnicos de forma multidisciplinar, para que exista uma proteção dos dados pessoais que serão tratados. Essas medidas devem incluir proteção contra acessos não autorizados, modificação dos dados, perdas ou qualquer forma de tratamento inadequado.

Qualquer pessoa que esteja presente em alguma fase do tratamento dos dados – incluindo operador, controlador e outras pessoas – deve garantir a segurança dos dados com os quais estão trabalhando, incusive após o término do tratamento, conforme o artigo 47 [2].

Caso ocorra algum tipo de problema com os dados dos titulares que possa causar danos ou possa trazer riscos aos mesmos, é de dever do controlador comunicar à ANPD o episódio. Conforme o parágrafo 1 do artigo 48, o aviso deve ser feito em tempo razoável, definido pela autoridade nacional, e deve conter, entre outros itens, as informações a respeito dos dados pessoais que foram afetados e dos titulares, os riscos relacionados ao incidente e as medidas que foram ou serão tomadas para minimizar ou reverter o prejuízo decorrente desse incidente [2].

Como dito no artigo 49 da LGPD, todo sistema que é utilizado para o tratamento de dados pessoais deve ser codificado de modo que atenda a todos os requisitos de segurança necessários, aos padrões de boas práticas e de governança previstos no texto e a outras regras que existirem [2].

Segundo o Art. 50 da Lei 13.709/2018, tanto controladores como operadores podem elaborar regras dentro dos tópicos de boas práticas no tratamento dos dados como em relação à governança da instituição. Podem também incluir nessas novas regras pontos como regime de funcionamento, normas de segurança, padrões técnicos, mecanismos para a redução de riscos, além de outros itens relacionados às operações feitas com dados pessoais.

Para que essas regras sejam estabelecidas devem ser levadas em consideração as operações realizadas e a natureza dos dados, a finalidade e os benefícios que serão o resultado do tratamento, de acordo com o parágrafo 1 do artigo 50.

A ANPD incentivará a adesão a padrões técnicos que ajudem a visualização pelos titulares de seus dados, como está escrito no Art. 51 [2].

Sobre a fiscalização a ser realizada e também a respeito das sanções administrativas que podem vir a ser aplicadas, o Art. 52 presente na seção I do capítulo VIII discorre que, caso venha a ocorrer que um agente de tratamento de dados cometa uma infração, esse fica sujeito a penas que devem ser executadas pela Autoridade Nacional. As penas são muitas, podendo variar desde uma simples advertência (esta que vem com um prazo para a implementação de melhorias na segurança) como também uma multa simples de até 2% (dois por cento) do faturamento da empresa, limitando-se a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, presentes nos itens 1 e 2 deste artigo, respectivamente. Da mesma forma, pode ocorrer uma multa diária, respeitando o item 2. Também deve ser informado publicamente sobre a infração uma vez que a mesma tenha sido confirmada, de acordo com o item 4 desse artigo. Essas são algumas das penalidades que podem vir a afetar quem não respeitar a LGPD [2].

Como pode ser analisado na LGPD, existe a peculiaridade em relação à proteção de dados pessoais por instituições públicas e privadas. A multa simples – de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração – e a multa diária, previstos pela Lei (Artigo 52) não são aplicáveis às entidades e instituições públicas. Apesar de as sanções financeiras não serem cabíveis sobre as instituições citadas anteriormente, elas deverão garantir a segurança dos dados pessoais dos titulares e atender os seus direitos previstos no Artigo 18 da Lei.

Inclusive os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento previsto no capítulo IV da Lei Geral de Proteção de Dados [10].

Como está descrito no Art. 53 da Lei 13.709, a ANPD é o órgão que cuidará das penalidades pelas infrações à Lei, através da um regulamento próprio. Todas as normas e metodologias que forem levadas em conta para o cálculo da multa devem ter sido publicadas previamente, e o documento contendo a descrição da multa deve ser de consulta pública. Já o artigo seguinte, 54, descreve sobre os procedimentos que serão aplicados caso uma multa diária seja aplicada [2].

Na seção seguinte e, consequentemente, no capítulo subsequente, são tratadas as informações a respeito da ANPD (Autoridade Nacional de Proteção de Dados). Todo o artigo 55 da Lei é referente à autoridade nacional. Conforme o mesmo, a ANDP é composta, de acordo com o Art. 55-D da Lei 13.709/19, por:

I. Conselho Diretor;
II. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
III. Corregedoria;
IV. Ouvidoria;
V. Órgão de assessoramento jurídico próprio;
VI. Unidades administrativas e unidades especializadas necessárias à aplicação da Lei.

Também é dito que o Conselho Diretor da autoridade nacional será composto por 5 diretores, sendo já incluído o Diretor-Presidente (Art. 55-D). Todos os membros do Conselho Diretor serão escolhidos e nomeados pelo Presidente, seguindo para aprovação do Senado, conforme parágrafo 1 do artigo prévio [2].

Em relação às responsabilidades da Autoridade Nacional, todas são expostas no artigo 55-J, sendo algumas delas:

- Zelar pela proteção dos dados pessoais, nos termos da Lei;
- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Fiscalizar e aplicar sanções em cada tratamento de dado que não obedeça à Lei;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- Garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento;
- Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais de desconformidade com esta Lei.

A seção II deste capítulo, intitulada “Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade”, possui apenas um artigo, o 58-A, o qual trata sobre o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Este conselho deverá ser composto por 23 membros, divididos entre outros órgãos do governo como Senado Federal, Câmara dos Deputados e Poder Executivo federal, entre outros. Como está descrito no Art. 58-B da LGPD, as responsabilidades do Conselho, adicionado através da Lei N° 13.853/2019, são: propor normas para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; desenvolver relatórios anuais sobre a execução das ações presentes na Política Nacional de Proteção de Dados; sugerir ações que a ANPD deva realizar, entre outras.

No dia 20 de outubro de 2020 o Senado aprovou os nomes indicados pelo Presidente para a composição da diretoria da Autoridade Nacional de Proteção de Dados. O cargo de diretor-presidente da ANPD, que faz parte do conselho diretor do órgão, foi aprovado para Waldemar Gonçalves Ortunho Junior, cuja formação é em engenharia eletrônica e pedagogia, e com pós-graduação em engenharia elétrica. Desde janeiro de 2019 ocupa o cargo de presidente da Telebras. Outros 2 nomes militares também foram nomeados, estes são Arthur Pereira Sabbat e Joacil Basilio Rael que, atualmente, são respectivamente o diretor do Departamento de Segurança da Informação do Gabinete de Segurança Institucional do Paraná e assessor da Telebras.

Outros dois nomes, dessa vez civis, foram indicados e aceitos. Miriam Wimmer e Nairane Farias Rabelo são, atualmente e nessa ordem, diretora de Serviços de Telecomunicações no Ministério das Comunicações e professora de direito, tecnologia e inovação em Brasília, e, advogada e sócia de um escritório de advocacia [33].

Todos os mandatos desse primeiro grupo variam de dois a seis anos, em contrapartida ao previsto na legislação que criou a entidade [34].

Em seu último capítulo, a LGPD possui seus artigos finais. O artigo 60 faz referência ao Marco Civil da Internet (Lei n° 12.965/2014 [32]), mais precisamente ao item 10 e 2 dos artigos 7 e 16, respectivamente. No primeiro, é definido que todos os dados pessoais fornecidos devem ser excluídos uma vez que ocorra o término da relação entre os envolvidos. Apenas quando previsto em Lei essa exclusão não deverá ser realizada. Em relação ao item 2 do artigo 16, este versa sobre a guarda

de dados que não sejam essenciais para a realização de uma aplicação na internet; agora, com a LGPD, isso é proibido.

O próximo tópico apresenta as classificações de dados conforme a LGPD.

3.3.1 Dados pessoais, dados sensíveis e dados anonimizados

Na LGPD não existem somente os dados pessoais, existem outras categorias além destes que são chamadas de dados sensíveis e dados anonimizados.

Pode-se definir dado pessoal como qualquer dado ou informação relacionados a pessoa identificada ou identificável. A União Europeia define dado pessoal como “dados relativos a uma pessoa singular identificada ou identificável”. Isso quer dizer que um dado ou informação se enquadra nessa categoria quando, a partir do mesmo, é possível a identificação, direta ou indireta, do indivíduo titular, conforme consta no Artigo 5, item 1, da LGPD [2]. Exemplos de dados pessoais são: nome, sobrenome, telefone, e-mail, RG, CPF, Passaporte, Carteira de Trabalho, Título de eleitor e endereço IP.

Em relação a dados sensíveis, a Lei os considera como qualquer informação que permita levar discriminação e preconceito ao seu titular. Um dado sensível sozinho pode não ter tanta relevância, mas ao ser combinado com um dado pessoal do titular pode ser capaz de comprometer a privacidade do mesmo. Alguns exemplos de dados sensíveis são: origem racial ou étnica, convicção religiosa, informações a respeito de saúde, afiliação política, dados genéticos ou biométricos, de acordo com o item 2 do artigo 5 da Lei [2].

Como um dado sensível pode causar prejuízo ao seu titular, a sua proteção deve ser mais rígida. No entanto, destaca-se que a LGPD determina o tratamento desses dados apenas em situações que são necessárias [30].

Quando um dado não permite que seu titular seja identificado, de forma tanto direta como indireta, o mesmo é classificado como dado anonimizado. De acordo com a Serpro um dado anonimizado é uma informação que um dia já teve titular, porém, através de processos de anonimização foi garantida a desvinculação da pessoa [19].

Um dado somente é considerado anônimo se não houver meios – técnicos ou quaisquer outros – que permitam reconstituir o processo pelo qual o dado passou e, assim, descobrir o titular original do mesmo, segundo item 3 do artigo 5 da LGPD [2].

Conforme consta no site do Planalto no texto da Lei N° 13.709/2018, um Dado Anonimizado é um “[...] dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento” [2] [19]. No artigo 12, é descrito que um dado anonimizado não é considerado dado pessoal para os fins da Lei N° 13.709/2018 [2].

Conforme o Guia de Boas Práticas da LGPD divulgado pelo Governo Federal ressalta, caso exista a possibilidade do dado anonimizado sofrer uma reversão em seu processo de anonimização, esse processo deixa de ser considerado assim e passa a ser considerado como pseudonimização [30].

3.3.2 DPO

Com a vinda da LGPD também haverá um novo profissional no mercado de trabalho. Esse cargo é o do DPO (*Data Protection Officer* – Encarregado da Proteção de Dados, em tradução livre), também chamado de Encarregado, como descrito no texto da Lei. De acordo com a Lei N° 13.709/2018, a partir do momento que a própria esteja em vigor, as instituições públicas e privadas devem ter alguém para cuidar da proteção dos dados de seus funcionários, colaboradores, clientes e usuários. Dentre as principais funções de um DPO estão:

- Porta voz entre a instituição e a ANPD (Agência Nacional de Proteção de Dados);
- Reportar aos titulares possíveis violações de seus dados e prestar esclarecimentos.

Um DPO pode tanto ser uma pessoa física como jurídica, e pode ser tanto um funcionário interno da instituição como alguém de fora. Uma vez que o Encarregado de Proteção de Dados seja escolhido, sua identidade e suas informações de contato devem ser divulgadas publicamente, visto que é ele quem as pessoas devem contatar caso acreditem ter encontrado algo de errado nos processos com seus dados. É dever dele aceitar reclamações, prestar esclarecimentos a clientes e usuários, e adotar medidas que visem à segurança dos dados, conforme explicado no artigo 41, parágrafo 2 da Lei [2].

A Secretaria do Governo Digital do Ministério da Economia publicou no Diário Oficial da União, na data de 20 de novembro de 2020, a Instrução Normativa 117, a qual em seu artigo 1°, parágrafo 1, inciso II, observa que o Encarregado de Dados Pessoais “[...] não deverá se encontrar lotado nas unidades de Tecnologia da Informação ou ser gestor responsável de sistemas de informação do órgão ou da entidade. ” [49].

Existe também outro tópico sensível em relação à escolha do DPO: se este será alguém interno da instituição ou se será alguém de fora. Caso seja alguém de dentro, essa pessoa já terá os conhecimentos a respeito da dinâmica de trabalho de dentro da instituição pública e/ou privada, e também conhecerá as pessoas com quem irá trabalhar. Se for uma pessoa externa, deve ser avaliado com mais critérios para garantir a segurança dos dados daquela instituição de forma que uma pessoa que não possui ligação não apresente riscos. [20] [21]

Para as atividades de tratamento dos dados existem alguns princípios presentes no artigo 6 do texto da LGPD:

- Finalidade: o tratamento dos dados somente pode ocorrer caso seu propósito seja legítimo e informados ao titular;
- Adequação: a finalidade do tratamento deve ser compatível com a informada ao titular;
- Necessidade: limitar o uso dos dados ao mínimo possível para a realização de determinada tarefa;
- Livre acesso: garantia aos titulares da visualização de fácil acesso e gratuita aos seus dados e como os mesmos estão sendo utilizados no tratamento e a duração;
- Qualidade dos dados: garantia de clareza e exatidão aos titulares;
- Transparência: garantir ao proprietário informações claras e precisas a respeito dos tratamentos aos quais seus dados são submetidos e também a respeito das pessoas responsáveis por este tratamento, respeitando os segredos comerciais e industriais;
- Segurança: fazer o uso de medidas para garantir a proteção dos dados pessoais e não permitir o acesso de pessoas não autorizadas

aos mesmos. Garantir que não ocorram situações acidentais de perda, alteração, destruição ou comunicação dos dados;

- Prevenção: empregar o uso de medidas para prevenir o dano ao dado;
- Não discriminação: impossibilidade de realização de tratamentos cujas finalidades sejam abusivas ou ilícitas;
- Responsabilização e prestação de contas: informação sobre as medidas tomadas para garantir a segurança dos dados assim como a eficácia destas providências.

A Agência Nacional de Proteção de Dados será um órgão fiscalizador e um meio de comunicação direto para pessoas (usuários, clientes, funcionários) que desejem criticar algo relacionado à proteção de seus dados pessoais de uma instituição pública ou privada que não esteja fazendo uso de boas práticas em seus sistemas [22].

Com a vigência efetiva da Lei caberá aos profissionais de T.I., assim como ao setor no qual trabalham, realizar todos os procedimentos de segurança tanto no armazenamento de dados pessoais como no tratamento desses e das informações geradas a partir dos mesmos.

Conforme artigo do site AlgarTech, é de responsabilidade da equipe de T.I. implantar e administrar os sistemas que controlarão dados. Outra responsabilidade da área de tecnologia da informação é “[...] diagnosticar, executar o plano de adequação à lei, e por acompanhar a eficiência das ações em todas as plataformas de entrada e saída de dados sensíveis de funcionários, parceiros, fornecedores e clientes no dia a dia” [57];

Com relação ao profissional de T.I., não importando se a Instituição à qual presta serviços é pública ou privada, de acordo com o artigo de Denis Zeferino do site Certifiquei, o papel deste colaborador é controlar os dados pessoais fazendo uso de mecanismos de segurança quando houver o tratamento dos mesmos [58].

Um dos principais fatores novos que deve ser incorporado ao design do software é a privacidade, a qual permite que a pessoa de posse dos dados tenha liberdade para visualizar e decidir se seus dados podem continuar a serem usados ou se há algum dado mais especifico que gostaria que não fosse mais utilizado e, assim, devido à decisão do proprietário, ter esse dado excluído.

Além de serem implementadas no desenvolvimento do software na instituição, essas novas diretrizes devem ser utilizadas também no modelo de negócios da mesma, uma vez que o software se baseia em como a instituição funciona. Logo, se ocorre uma mudança no sistema, deve haver também uma mudança no plano de negócios da instituição para que ambos estejam em conformidade [23].

A seguir são apresentadas metodologias com foco em privacidade.

3.4 *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*

Para a adequação, é interessante o profissional responsável conhecer e aplicar no desenvolvimento do sofware o *Privacy by Design*, conforme é apresentado no artigo do site Ostec. O *Privacy by Design* é uma metodologia na qual a proteção dos dados deve ser pensada desde a concepção do sistema. Desde a fase de discussão a respeito dos requisitos funcionais e não funcionais a proteção dos dados é um requisito não funcional obrigatório a todos os sistemas a partir do momento em que a Lei N° 13.709/2018 foi aprovada [24].

Privacy by Design é uma metodologia criada nos anos 90 no Canadá. Especialistas do governo naquela época já imaginavam que no futuro haveria uma coleta volumosa dos dados dos indivíduos, o que de fato ocorre atualmente. Logo, foi criada esta metodologia para que houvessem regras que pudessem ser aplicadas nas instituições. Hoje, o *Privacy by Design* tem seus princípios incorporados na GDPR e na LGPD, embora não exista referência explícita ao termo. O conceito dita que instituições públicas e privadas apliquem as técnicas presentes na metodologia em todo o produto e/ou serviço, ou seja, que a proteção dos dados e das informações do cliente estejam presentes desde a criação até seu futuro desligamento, durante todo seu ciclo de vida [24].

Existe também o *Privacy by Default*, um conceito que significa que sempre que um software for disponibilizado, suas configurações de privacidade mais seguras devem vir aplicadas por padrão. O usuário não precisa realizar nenhuma configuração para chegar ao estado mais seguro de proteção; se precisar tomar alguma ação, então esse conceito será violado [28].

Esses dois conceitos são muito utilizados na GDPR e serão muito usados também para a adequação na LGPD [24] [28].

Assim como este é um requisito obrigatório, existem também determinadas características que o profissional que tratará do desenvolvimento deve possuir, assim como o software a ser construído deve apresentar [25]. Dentre elas estão:

- Ser proativo;
- A privacidade com a qual os dados serão tratados será sempre máxima;
- Solução que está sendo desenvolvida deve ser 100% pensada no usuário;
- A segurança sob a qual os dados estarão sujeitos será de ponta a ponta.

Os dados pessoais que já estão no banco de dados das instituições públicas e privadas deverão passar por uma atualização para enquadramento nas novas regras uma vez que, mesmo coletados antes da entrada em vigor da LGPD, eles são considerados como em situação de armazenamento [2].

Uma das principais dificuldades que podem ocorrer nas instituições públicas e privadas durante o processo de adaptação à Lei Geral de Proteção de Dados é o levantamento dos dados que possuem [26]. É importante identificar nas instituições públicas e privadas quais dados são coletados, com quais finalidades, onde estão localizados e o nível de proteção necessário e se ainda são necessários [27].

É apresentado a seguir o porquê da manutenção de um sistema ser tão crítica, e quais pontos são interessantes observar durante a atualização de um software.

3.5 MANUTENÇÃO

Por ser uma Lei que tem aplicação a todo ambiente de T.I. e todo sistema que armazena dados, é necessário que ocorram manutenções para que todos fiquem de acordo com a nova regulamentação [2].

No livro “Engenharia de Software – Uma Abordagem Profissional”, de Roger S. Pressman, o autor escreve que a manutenção de um software é uma das partes que mais consomem tempo e recursos financeiros. Não é raro que uma companhia empregue de 60% a 70% de seus recursos em manutenção de seus softwares [7]. Logo, no planejamento da construção do software, deve-se adicionar mais um tópico

a ser implementado: o da conciliação com a nova legislação. Isso apenas para novos softwares; para aqueles já existentes deverá ser feita uma manutenção obrigatória de forma que fique de acordo com as novas políticas de proteção de dados.

Conforme Pressman apresenta em seu livro [7], Manny Lehman e seus colegas estudaram nos últimos 30 anos softwares industriais e desenvolveram a *teoria unificada para a evolução do software* (*unified theory for software evolution*). Desse estudo derivaram algumas leis, como:

- A Lei da Mudança Contínua (1974): softwares que foram implementados num contexto de mundo real evoluirão com o tempo, dessa forma devem ser adaptados ou ao longo do tempo serão menos eficientes e poderão não realizar mais a atividade que deviam fazer de forma eficaz;
- A Lei da Complexidade Crescente (1974): à medida que um software evolui, sua complexidade também aumenta, exceto se houver um projeto para mantê-la ou reduzi-la;
- A Lei do Crescimento Contínuo (1980): o conteúdo de sistemas deve ser sempre que possível ampliado ao longo de sua existência para que seu trabalho seja feito de forma correta e garanta a satisfação do usuário;
- A Lei da Qualidade em Declínio (1996): a qualidade dos sistemas decairá caso não ocorram mudanças e adaptações do ambiente operacional.

Conforme exposto por Gerald Berns [7] “[...] manutenibilidade e clareza de programa são conceitos paralelos: quanto mais difícil for entender um programa, mais difícil será mantê-lo”. Essa frase de Berns mostra o quanto a manutenção é importante.

Um software cuja manutenção pode ser considerada “fácil” é aquele que apresenta modularidade eficaz, utiliza padrões de projeto, entre outras técnicas da Engenharia de Software, para que não somente a manutenção seja simplificada, mas todo o percurso desde o seu desenvolvimento até sua aposentadoria [7].

Todas essas informações têm como principal propósito a suportabilidade do software, cuja definição escrita por Pressman é [7] “[...] a capacidade de suportar um sistema de software durante toda a vida útil do produto. Isso implica satisfazer quaisquer necessidades ou requisitos, mas também a provisão do equipamento, infraestrutura de suporte, software adicional, serviços de conveniências, mão de obra ou qualquer outro recurso necessário para manter o software operacional e capaz de satisfazer suas funções.”

No campo da Engenharia de Software existem diversos tipos de manutenção que um software pode sofrer. Manutenção “corretiva”, “adaptativa” e “perfectiva” são apenas nomes dados a mudanças feitas no software, porém de acordo com Sommerville, não existe uma distinção clara desses tipos [8].

Já de acordo com Wazlawick (p. 320) a manutenção corretiva é o nome dado às mudanças feitas no software de modo que seja possível corrigir possíveis defeitos já identificados que podem acarretar erros no software. Essa categoria pode ser dividida em duas subcategorias: 1) manutenção para correção de erros conhecidos e 2) manutenção para detecção e correção de novos erros.

A manutenção adaptativa é a mudança para que o software fique de acordo com as necessidades do cliente pelo máximo de tempo possível. Essa manutenção vem diretamente das Leis da Lehman, indicando que no decorrer do tempo podem haver novos requisitos por parte dos clientes. Também leis e normas são aprovados e o software deve ser atualizado para ficar de acordo (nesse caso, de acordo com as novas normas da LGPD). Além do mais, quando novas tecnologias são lançadas, sua utilização pode trazer benefícios ao sistema já em operação.

A manutenção perfectiva é realizada geralmente para que o sistema tenha um desempenho melhor ou que faça seu trabalho de modo mais eficiente do que a concorrência. Tal mudança é crítica em softwares como jogos e sistemas de controle em tempo real [9].

Por fim, o último tipo de manutenção que Wazlawick cita em seu livro é a manutenção preventiva, a qual é realizada de modo que um possível erro possa ser evitado. Um exemplo que o autor cita é um sistema que suporta até 50 acessos, mas que possui cerca de 20 a 30 acessos simultâneos; uma manutenção preventiva nesse caso seria aumentar esse limite de acessos para 100, 200 ou até mesmo 500 acessos simultâneos, de modo que o limite seja expandido evitando o risco de colapso no sistema em um futuro próximo [9]

Existem vários motivos pelos quais realizar uma mudança no software após o desenvolvimento, além de ser mais caro, torna-se mais difícil. Como cita Sommerville [8]:

- Estabilidade da equipe: dificilmente a mesma equipe que fez o desenvolvimento do software será a equipe que realizará a manutenção, logo, as pessoas responsáveis podem não entender o sistema nem as decisões tomadas para que o mesmo fosse construído daquela forma;
- Más práticas de desenvolvimento: geralmente o contrato de desenvolvimento do software é separado do contrato de manutenção. Dessa forma, não existe incentivo para a equipe de desenvolvimento escrever um software manutenível, e se for possível cortar custos de forma que a manutenção futura seja piorada, esse corte será feito;
- Qualificação pessoal: para os engenheiros de software a manutenção tem uma imagem pobre e é vista como um processo menos qualificado que o desenvolvimento, logo, equipes mais jovens e com menos experiência são alocadas para tal atividade. Caso o sistema seja muito antigo, pode ser necessário que essa equipe mais nova aprenda a linguagem para somente então começar a realizar a manutenção;
- Idade do programa e estrutura: após várias alterações no software, o mesmo tende a se degradar. Logo, sua estrutura pode ser menos inteligível do que quando foi lançado. Suas documentações podem estar desatualizadas e pode ser difícil encontrar o local certo onde fazer a manutenção e o que será afetado por tal mudança.

Conforme descrito por Jason Schreier em seu livro *Blood, Sweat and Pixels*, alguns desenvolvedores de software acreditam que as correções de problemas e *bugs* presentes no software acontecem apenas após o seu lançamento. Esse pensamento ocorreu no lançamento do *game* Diablo III em 2012, desenvolvido pela Blizzard Entertainment. Mesmo tendo levados anos para que o desenvolvimento fosse concluído, e corrigindo todo tipo de problema que aparecesse durante esse

tempo, não foi suficiente para que o software estivesse totalmente pronto em seu lançamento, em maio de 2012.

Alguns funcionários que trabalharam na produção do software disseram em entrevistas para o livro que todos os *bugs* corrigidos durante o desenvolvimento do game foram os encontrados por sua equipe e os testadores, porém, essa equipe era de cerca de 400 pessoas. Uma vez que o software foi lançado mundialmente, milhões de pessoas puderam utilizar o produto, e assim milhares de outros problemas e *bugs* começaram a serem reportados [6].

Esse é um exemplo de como a manutenção é importante, pois apesar do desenvolvedor e toda sua equipe acreditarem que seu produto está perfeito e em ótimas condições para ser lançado, o que realmente importa é a opinião do cliente a respeito daquilo que passou por anos consecutivos de desenvolvimento [6].

O próximo capítulo apresenta o estudo de caso em relação à LGPD, realizado na Universidade Federal do Paraná.

4 ESTUDO SOBRE A LGPD EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR: UNIVERSIDADE FEDERAL DO PARANÁ

Foi decidido que o objeto de análise deste trabalho seria a Agência de Tecnologia da Informação e Comunicação (AGTIC) da Universidade Federal do Paraná para identificação do estágio em que se encontra a implantação das regras necessárias para a LGPD.

Neste capítulo serão apresentadas as ações que a AGTIC já fez, tem realizado e quais serão feitas para tratar da segurança da informação e da LGPD.

4.1 AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (AGTIC)

A Agência de Tecnologia da Informação de Comunicação (AGTIC) é o órgão da UFPR cujas responsabilidades incluem a direção, planejamento, desenvolvimento, execução, suporte e monitoramento de atividades relacionadas à tecnologia de informação e comunicação [35]. Conforme consta na Resolução N° 45/19-COPLAD, artigo 3, item 1, as atribuições que são de responsabilidade da AGTIC incluem a promoção do uso sustentável, eficiente e seguro de todos os recursos de tecnologia da informação e comunicação, estes podendo ser pessoas,

infraestrutura, equipamentos e software, que foram designados para estarem sob a responsabilidade da agência. Também é de responsabilidade da AGTIC executar e monitorar o Plano Diretor de tecnologia da informação e comunicação (PDTIC), assim como realizar sua revisão e sua retificação para que fique de acordo com as estratégias da instituição. Além disso, deve prestar apoio às atividades de ensino, pesquisa e extensão, assim como apreciar todos os projetos que envolvam TIC (tecnologia da informação e comunicação) da universidade com o intuito de racionalização e otimização de recursos, conforme item 3 e 4 do artigo 3 da Resolução [35].

Também presente no mesmo artigo, nos itens 5 e 7, a AGTIC deve sempre buscar soluções que automatizem e/ou otimizem processos, da mesma forma que todos os dados, redes e sistemas armazenados sob sua responsabilidade devem sempre estar disponíveis de forma confiável e segura. Os itens 11 e 12 referem-se ao dever da Agência de promover a coordenação de processos de transformação digital e o desenvolvimento de softwares institucionais.

Presente na Seção II, artigo 5 da Resolução N° 45/19-COPLAD, descreve-se que é dever da Unidade de Segurança, Riscos e Governança de TIC (uma unidade subordinada à Diretoria Executiva da AGTIC) a “promoção, orientação, validação e controle de ações em segurança da informação, processos, projetos e riscos, em conformidade com o PDTIC” [36].

Na Seção VI da Resolução referida previamente, temos o artigo 12, item 6, o qual discorre que uma das responsabilidades da Coordenadoria de Soluções de Software é: “[...] propor tecnologias e arquiteturas de desenvolvimento e de banco de dados adequadas às necessidades da UFPR”. Também presente no mesmo artigo, no item 14, encontra-se a obrigação da AGTIC de propor projetos e atividades cujo objetivo seja a adoção de políticas e normas de TIC e Segurança da Informação [36].

Na reunião que ocorreu em março de 2020 foi discutido sobre as regras que as instituições públicas de educação, em especial as Universidades, devem seguir, suas penalidades (uma diferença em relação à LGPD aplicada em instituições privadas é que no setor público não existe a multa financeira), entre outros assuntos. Outro tópico discutido foi de que, até então, o Governo Federal não possuía nenhum tipo de padrão ou protocolo que pudesse ser seguido para a implementação e a implantação das normas da LGPD nas Universidades Públicas. Como não existe

esse padrão, cada instituição deve fazer por conta própria os seus estudos e verificar o estado atual de seus dados, tanto de servidores técnico administrativos como professores e de alunos, para que somente depois sejam estruturadas as mudanças necessárias.

Em 22 de setembro de 2020 o Governo Federal disponibilizou a página de Guias Operacionais para adequação à LGPD, contendo documentos que devem auxiliar na implantação das novas regras. Na página existem documentos relacionados a diversos tópicos necessários em relação à Lei N° 13.709/2018, como: Programa de Governança em Privacidade, Inventário de Dados Pessoais, Termo de Uso, Avaliação de Riscos, Adequação de Contratos e Relatório de Impacto de proteção de dados (RIPD). O site informa que as guias operacionais disponíveis para consulta serão periodicamente atualizadas [51].

Na UFPR existem três categorias: alunos, professores e servidores técnico-administrativos. Ainda há também servidores terceirizados presentes na Universidade. Cada categoria apresenta suas particularidades e todas devem ser incluídas nas ações de mudança de cultura que ocorrerão. Para Paulo Leão, em artigo publicado no site da Serpro, “[...] as organizações públicas e privadas estão diante de uma significativa mudança cultural em relação à proteção e privacidade dos dados pessoais” [59].

Com relação à Lei N° 13.709/2018, foi na data de 8 de julho de 2020 que o comitê de planejamento da implantação de políticas de LGPD foi instaurado pela Universidade Federal do Paraná para iniciar as adaptações necessárias (Portaria N° 1130/Reitoria, de 08/07/2020).

Um exemplo de situação que mostra que a LGPD deve ser implantada de forma correta juntamente com outras medidas de segurança e privacidade (como uma política ou normas) ocorre quando, no contexto da UFPR ou de uma Universidade Pública, um professor posta um material em seu site sem creditar sua autoria. Neste caso, com uma campanha de conscientização sobre as normas da LGPD e de Políticas internas, essa situação não ocorreria.

4.2 RESOLUÇÃO N° 21/14-COPLAD

Em 24 de setembro de 2014 a Resolução de número 21/14-COPLAD entrou em vigor, bem como a Política de Segurança da Informação da Universidade

Federal do Paraná (PSI/UFPR) e todos os seus 29 artigos para a segurança de todo e qualquer tipo de informação dentro da Universidade [42].

Na Resolução existe a definição de vários termos relacionados à segurança de informação, assim como na LGPD. Mesmo sendo mais antiga que as definições presentes no texto da Lei N° 13.709/2018, é possível perceber que as normas publicadas em 2014 são atuais e podem ser vistas dentro do contexto analisado neste momento.

Conforme consta no artigo 1 da PSI/UFPR, além de serem definidas regras em âmbito geral e também em grau mais específico, são caracterizados procedimentos complementares cujos objetivos são a proteção de informações, a disseminação e a utilização das mesmas dentro da Instituição. O artigo seguinte reitera os propósitos presentes na Resolução de forma a explicitar que seus objetivos são: a garantia da autenticidade, da confidencialidade, da disponibilidade e da integridade das informações e dados desenvolvidos e armazenados pela UFPR. Todas essas informações devem seguir cinco diretrizes, conforme constam nos itens 1 a 5 deste mesmo artigo, que são:

I- Observância da publicidade como preceito geral e do sigilo como exceção;
II- Divulgação de informações de interesse público, independentemente de solicitações;
III- Utilização de meios de comunicação viabilizados pela tecnologia da informação;
IV- Fomento ao desenvolvimento da cultura de transparência na administração pública;
V- Desenvolvimento do controle social da administração pública.

Conforme é citado no artigo 4 e em seus quatro itens, a segurança da informação na Universidade Federal do Paraná engloba aspectos humanos, físicos e tecnológicos juntamente com os seguintes princípios:

- Confidencialidade: caracteriza que a informação somente esteja à disposição para indivíduo, órgão ou entidade autorizada;

- Disponibilidade: propriedade de que os dados estejam disponíveis e possam ser utilizados para um indivíduo, entidade, órgão ou sistema desde que o mesmo possua autorização;
- Integridade: a informação deve estar em sua forma original, sem nenhum tipo de alteração, salvo quando a alteração é autorizada;
- Autenticidade: o dado foi desenvolvido ou sofreu qualquer tipo de processamento (modificação ou destruição) por pessoa física ou órgão autorizado.

O Centro de Computação Eletrônica (CCE) – atualmente AGTIC – através do Departamento especializado em Segurança da Informação, é o órgão cujas responsabilidades são coordenar e acompanhar a implementação da Política de Segurança da Informação na Universidade Federal do Paraná, conferir e aprovar processos fundamentais para a implementação da mesma, realizar avaliações periódicas a respeito das práticas de segurança da informação adotadas, e também é sua obrigação a constituição de uma equipe para tratamento de incidentes caso venha a ocorrer qualquer problema.

Todas as medidas e regras adotadas devem passar pelo processo de planejamento, aplicação, implementação e devem ser regularmente avaliadas sob a ótica dos objetivos da Instituição e os possíveis riscos para as atividades realizadas na Universidade, de acordo com o artigo 8 [42].

Conforme consta no artigo seguinte da Resolução N° 21/14-COPLAD, qualquer interessado tem o direito de acessar a informação, desde que o pedido seja realizado por meio legítimo e no mesmo deve estar explícita a identificação do requerente e a especificação do dado requerido. Após feito o pedido, o órgão ou unidade terá de conceder ou não o acesso à informação sem tardar. Uma vez que não seja possível a concessão do acesso imediato aos dados, o órgão ou entidade que recebeu o pedido tem um prazo de vinte dias para informar a data, local e modo de realização da consulta. Esse prazo pode ser prorrogado por mais dez dias, mas somente por meio de justificativa.

Caso a resposta seja de que não é possível conceder a informação ao requerente (pois a informação desejada é parcial ou totalmente sigilosa) deve ser informado sobre as possibilidades de recursos, prazos e condições para sua nova tentativa, caso deseje [42].

Todas as informações elaboradas e mantidas pela Universidade Federal do Paraná (UFPR) deverão ser classificadas de acordo com seu nível de confidencialidade, disponibilidade, integridade e prazo de retenção, como está escrito no artigo 14. O prazo de retenção é definido junto ao Sistema de Acervos e Arquivos da UFPR, e a autorização para acesso e potencial uso dessas informações contidas ou produzidas dentro da UFPR será controlada de acordo com seu nível de classificação.

Em relação ao nível de confidencialidade das informações, as mesmas serão classificadas nos seguintes níveis:

- Públicas: dados e informações que podem ser compartilhados com todos;
- Restritas: dados e informações que, por seu conteúdo ou conforme foi determinado pela Universidade, podem apenas ser compartilhados com um número menor de pessoas;
- Sigilosas: nesse nível são classificadas informações que, devido a alguma lei, interesse público ou para não acarretar danos a direitos de indivíduos, têm seu acesso restrito;
- Pessoais: informações relacionadas a vida, honra e imagem de uma pessoa.

Uma vez que uma informação nova deva ser classificada, o critério para encontrar seu correto nível de sigilo deve ser sempre o mais abrangente possível, isto é, o que torne a informação mais acessível a todos [42].

Conforme citado na Resolução N° 21/14-COPLAD, dentro do nível das informações sigilosas existe uma classificação na qual podem ser categorizadas: informações reservadas, informações secretas e informações ultrassecretas. Cada nível possui um período de restrição pelo qual deve passar antes de se tornar público: 5 (cinco) anos para informações reservadas, 15 (quinze) anos para secretas e 25 (vinte e cinco) para ultrassecretas, conforme consta no quarto parágrafo do artigo 15.

Os dados e informações relacionados às pesquisas que serão desenvolvidas dentro da Universidade e corretamente registradas na Pró-Reitoria de Pesquisa e Pós-graduação (PRPPG) serão automaticamente classificados como informações

reservadas. Uma vez que ocorra a publicação dos resultados ou que seja realizada uma defesa pública de trabalhos finais de cursos, dissertações ou teses, a classificação prévia é cancelada [42].

Dado que uma nova informação é desenvolvida ou é fornecida para armazenamento na Universidade, é de responsabilidade do gestor da informação fornecer sua classificação de confidencialidade. Quando houver a classificação, deve-se observar todos os controles, tanto administrativos como tecnológicos, assim como quais serão os grupos de pessoas que poderão ter ou não acesso. Caso a classificação adquirida pela informação seja sigilosa ou restrita, é uma obrigação do gestor informar quem ou quais setores ou projetos ou unidades da Universidade possuem permissão para acessá-la, conforme consta no parágrafo 2 do Artigo 16 [42].

A qualquer momento a informação pode sofrer uma reclassificação em seu nível de confidencialidade, sendo esta ação realizada pelo gestor da informação ou outra autoridade competente. Essa mudança no nível de confidencialidade pode ser feita por iniciativa própria do gestor ou pode ser pedida através de uma solicitação, esta feita por qualquer usuário. Caso ocorra a alteração, o custodiante da informação deve ser informado o mais rápido possível [42].

O Artigo 19 da Resolução N° 21/14-COPLAD detalha informações a respeito das consequências em relação à disponibilidade ou não dos dados desenvolvidos ou custodiados pela UFPR. Existem três níveis de impacto: 1) baixo, quando a indisponibilidade dos dados não irá comprometer em nada os objetivos e imagem da Universidade, bem como não acarretará nenhum tipo de perda financeira; 2) médio: quando pode comprometer a imagem, a produtividade e as decisões tomadas para que os objetivos da Universidade possam ser cumpridos, mas que de forma alguma inviabilizem essas atividades ou causem qualquer tipo de perda financeira, e; 3) alto: quando a indisponibilidade dos dados pode vir a comprometer a imagem da Universidade severamente e suas operações de forma vital ou causar perdas financeiras.

Em relação à classificação de integridade de uma informação produzida ou custodiada pela Universidade, ela é feita a partir do impacto que um processamento (alteração, inclusão ou exclusão) indevido ou não autorizado possa refletir na imagem ou nas operações da UFPR [42].

Novamente, a classificação sobre o impacto em perda de integridade é feita em três níveis, conforme artigo 21: 1) baixo: quando o processamento da informação não compromete a imagem, nem as operações realizadas dentro da Universidade e não causará perda financeira; 2) médio: pode comprometer a imagem da UFPR, as decisões tomadas, assim como a produtividade das operações, porém sem necessitar que as mesmas parem ou que causem prejuízos financeiros à Universidade, e, por fim; 3) alto: caso ocorra a perda de integridade das informações desse nível custodiadas ou desenvolvidas na UFPR, irá comprometer a imagem e as operações vitais da Universidade, assim como também pode causar perda financeira severa [42].

Outras responsabilidades do gestor de informação incluem deveres como adotar todo e qualquer procedimento para garantir a segurança da informação, estabelecer regras a respeito de quem pode acessar aquela informação bem como os procedimentos necessários para a visualização da mesma. Caso uma informação seja recebida de uma pessoa física ou jurídica externa, medidas de segurança definidas juntamente com quem a forneceu serão acrescentadas à informação, como está escrito no artigo 22 [42].

Os servidores são os profissionais que têm entre as suas obrigações a atualização constante dos bancos de dados de forma que sempre estejam corretas as informações presentes, assim como informar imediatamente à ouvidoria da Universidade Federal do Paraná caso seja detectado qualquer nível de inconsistência em qualquer informação de seu setor. Mensalmente, a ouvidoria da UFPR encaminhará ao COPLAD (Conselho de Planejamento e Administração) as ocorrências registradas estruturadas por assunto, e também enviará os fatos que aconteceram para sua respectiva unidade [42].

O custodiante da informação deve garantir que qualquer informação sob sua posse deve estar segura conforme as especificações estabelecidas pelo gestor da informação. Deve também informar o mais rápido possível ao gestor caso detecte algum tipo de problema que possa vir a comprometer a segurança da informação que está sob sua responsabilidade. Caso perceba que existe algum tipo de limitação para o cumprimento das normas estabelecidas pelo gestor da informação para a segurança da mesma, o custodiante deve informar para que o gestor analise se determinada restrição deve ser suspensa ou não sem prejudicar o sigilo do dado, conforme escrito no Artigo 23 da Resolução N° 21/14-COPLAD.

No tocante à segurança da informação, compete aos respectivos dirigentes das unidades e demais chefias da Universidade Federal do Paraná fazer com que seus usuários e colaboradores compreendam os conceitos e práticas em relação à segurança da informação, integrar ao dia a dia de trabalho de sua unidade ou área projetos cujo caráter seja de segurança da informação, assim como, caso ocorra qualquer tipo de comprometimento de segurança de alguma informação, atuar de forma a responsabilizar o usuário ou colaborador sob sua supervisão através das medidas administrativas necessárias e ações corretivas [42].

Indicado pelo Reitor, o Gestor de Segurança da Informação, deve arcar com algumas responsabilidades, de acordo com o artigo 25, itens 1 a 4. Os deveres do gestor são:

- Caso ocorra algum comprometimento de alguma informação, o Gestor de Segurança da Informação deve acompanhar as investigações e avaliações dos danos causados devido à quebra de segurança;
- Estimular o conhecimento da segurança da informação na Universidade Federal do Paraná;
- Trabalhar juntamente com o DSInf (Departamento de Segurança da Informação) em investigações e tratamentos de casos de segurança da informação dentro de UFPR;
- Estudar e sugerir novos recursos que sejam necessários para as ações de segurança da informação na Universidade.

Contratos que devem ser firmados pela Universidade Federal do Paraná com instituições tanto públicas como privadas devem obedecer, na medida do possível, a todos os regulamentos presentes na Política de Segurança da Informação da Universidade Federal do Paraná. A utilização dos recursos tecnológicos de T.I. da UFPR deverá ser seguida por normas previamente estabelecidas. Caso alguma das normas presentes na Política de Segurança da Informação da Universidade Federal do Paraná não seja seguida, pode vir a originar penas, estas presentes na legislação aplicável, aos culpados por tal conduta.

4.3 LGPD EM 2020 NA UFPR

Em 8 de julho de 2020 a UFPR instaurou, a partir da Portaria N° 1130/Reitoria, o comitê para planejamento de implantação da LGPD, e com a Portaria N° 1393/Reitoria, de 1° de outubro desse mesmo ano, nomeou seu Encarregado de Proteção de Dados Pessoais, o DPO da Instituição.

Em e-mail enviado aos professores e servidores técnico-administrativos da Universidade, foi dito no Ofício anexo que estaria sendo contratada uma empresa especializada para que a mesma prestasse auxilio no processo de adequação da Universidade à nova Lei. Segundo informações do Encarregado de Dados Pessoais, a empresa terceirizada estava na fase de contratação durante a escrita desta pesquisa, com previsão de que a prestação desses serviços iniciasse ainda no ano de 2020 [37].

Na última atualização possível da informação antes da conclusão desta pesquisa, a empresa terceirizada foi contratada e sua primeira reunião com a AGTIC, para orientação, seria realizada na semana de 14 a 18 de dezembro de 2020 [48].

A AGTIC é o órgão responsável pela implantação da Lei N° 13.709/2018 juntamente com o comitê para planejamento de implantação da LGPD na Universidade Federal do Paraná.

Segundo o Ofício enviado aos docentes e demais servidores e colaboradores da Universidade, estes são informados que devem ficar atentos à mudança de cultura em relação a dados pessoais dentro da UFPR. Todos os que possuem dados pessoais e trabalham com eles devem ter cuidados com os mesmos. O compartilhamento desses dados somente pode ocorrer quando houver a autorização dos titulares.

Todos esses cuidados devem ser tomados tanto em relação a documentos físicos como digitais. É salientado também que não devem ser deixados esses dados em locais externos à UFPR, como e-mails ou nuvens não-institucionais.

Para que seja iniciada essa mudança de pensamento, com instruções de como executar as atividades a partir da mudança de cultura, foi criado um FAQ (*Frequently Asked Questions*) com dúvidas que podem vir à tona quando houver algum tipo de coleta ou tratamento de dado pessoal dentro da Universidade.

Foi criado também o TERMO DE PRIVACIDADE DO PORTAL DO CANDIDATO VESTIBULAR UFPR 2020/2021, no qual diversas informações a respeito dos dados coletados, quando serão coletados e quais as suas finalidades, são apresentadas. São expostas algumas das razões pelas quais são coletados os dados no Portal do Candidato e na Ficha de Inscrição que incluem, entre outras, cadastro do candidato e identificação do formulário de inscrição do candidato no vestibular. É dito também que todos os dados que são coletados no momento da inscrição somente serão compartilhados com a Pró-Reitoria de Graduação (PROGRAD) caso o candidato venha a ser aprovado e tenha sua matrícula confirmada para, assim, integrar o sistema acadêmico [11].

Além disso, são informadas as medidas de segurança tomadas pela UFPR para com os dados dos candidatos. São utilizadas senhas individuais para o acesso, algoritmos de criptografia estão presentes e o banco de dados possui camadas de segurança. Dicas para o próprio candidato cuidar de seus dados e não tornar-se vítima de golpes estão presentes no documento também [11].

O armazenamento dos dados é necessário, pois é preciso para que ocorra a viabilidade do processo seletivo e o cumprimento a Legislação Educacional, assim como atividades estabelecidas pelo Ministério da Educação (MEC). As informações são armazenadas em servidores próprios da UFPR, do Núcleo de Concursos, com tecnologias de segurança e o prazo de armazenamento em acordo com a Portaria MEC 1224/2013 [11].

No documento são constatados os direitos do titular que, utilizando uma requisição, pode confirmar a existência do tratamento dos dados, o acesso aos mesmos, corrigir algum dado que venha estar errado por alguma razão, entre outros, sendo todos presentes na Lei [11].

Também presente no termo estão todas as informações sobre cada dado requerido durante o processo de cadastro e inscrição, assim como são informados todos os valores possíveis para cada campo e sua finalidade.

Também no ano de 2020 foram desenvolvidas novas políticas que envolvem três assuntos muito relevantes para a LGPD: controle de acesso, uso de recurso de tecnologia da informação e comunicação e privacidade dos dados.

A Política de Controle de Acesso, datada do dia 2 de setembro de 2020, em sua versão de implantação, tem por objetivo “[...] estabelecer diretrizes para implementação de controles de acessos físicos e lógicos aos recursos de TIC

(Tecnologia da Informação e Comunicação), relativos à Segurança da Informação, na Universidade Federal do Paraná, em conformidade com as necessidades institucionais e legais". Todos os recursos englobados por essa política são ofertados e gerenciados pela AGTIC, assim como aqueles de outras unidades de TIC da UFPR. Qualquer usuário de recursos de T.I. na esfera da UFPR deverá seguir as informações presentes nessa norma, que compreende docentes, servidores, estudantes, entre outros [38].

Qualquer dado ou equipamento sob a gerência da AGTIC e/ou que está submetido a essa política deve ter seu acesso monitorado para que sempre seja feito de forma segura e responsável, e somente os usuários que têm vínculo ativo com a Universidade Federal do Paraná poderão pedir acesso aos dados. Quais dados serão concedidos e quais não serão dependerá da função que o solicitante tem dentro da Instituição, e este acesso somente será concedido caso ocorra a assinatura do Termo de Responsabilidade. Dependendo do tipo de recurso de TIC, pode vir a ser necessária a realização de procedimentos adicionais de autorização. Será feita pelo Gestor do Recurso a concessão do recurso requisitado [38].

Para que o acesso seja concretizado deverá ser utilizada senha pessoal, esta criada pelo Gestor do Recurso seguindo algumas premissas como:

- Conter no mínimo 8 caracteres, utilizando letras maiúsculas, letras minúsculas, números e caracteres especiais;
- Toda senha utilizada deverá trafegar na rede de forma criptografada;
- As senhas não devem durar mais de um ano, e devem ser alteradas dentro desse prazo.

Os usuários que farão uso dos dados terão as responsabilidades definidas na política, como: a obrigação do usuário manter-se informado sobre as regras atuais e qualquer tipo de alteração nas mesmas e na Política de Controle de Acesso; não compartilhar suas informações de acesso a terceiros; utilizar os recursos da instituição para e-mails e não o pessoal; informar o Gestor do Recurso ou a AGTIC a respeito de qualquer erro ou fragilidade de segurança detectada; não expor os dados a que tem acesso a pessoas não autorizadas, e manter seus dados atualizados e coerentes [38].

Além das responsabilidades dos usuários, a política também estabelece os deveres das chefias e das autoridades responsáveis, as quais são: assegurar que os servidores e colaboradores tenham conhecimento da Política de Controle de Acesso, assim como esses tenham acesso seguro aos recursos de TIC necessários; fornecer documentos que confirmam o vínculo ativo de um usuário sob sua responsabilidade, uma vez que esta for requisitada, entre outros.

Os Gestores de Recursos, assim como as chefias e os usuários, têm obrigações que incluem autorizar o acesso de funcionários a seus recursos e, caso julgue necessário, deve requisitar a alteração, bloqueio ou cancelamento de acesso. Além disso, uma vez que o término do serviço ocorra, deve solicitar o cancelamento de acesso [38].

A direção da AGTIC deve sempre manter essa política atualizada, assim como divulgar para a comunidade da UFPR. Em caso de mau uso dos recursos concedidos, o acesso poderá ser bloqueado ou até mesmo cancelado, e as informações sobre a infração devem ser fornecidas pelo Gestor do Recurso às autoridades que julgarão quais ações deverão ser tomadas [38].

Outra política desenvolvida na UFPR no ano de 2020 foi a Política de Uso de Recursos de TIC, sendo que sua versão de implantação é datada do dia 26 de outubro de 2020. Esta tem por objetivo estabelecer as normas sobre a utilização dos recursos, tanto físicos como lógicos, de tecnologia da informação e comunicação no âmbito da UFPR, a fim de reduzir os riscos que venham a ser causados por uso indevido, além de minimizar as ocorrências de ameaças e incidentes que possam comprometer a segurança da informação e o patrimônio da instituição, sempre de acordo com as necessidades legais e da Universidade. Deve ser aplicada a todos os recursos de TIC da UFPR e suas normas devem ser seguidas por todos os usuários desses recursos no âmbito da Universidade [39].

Todos os recursos de TIC fornecidos pela UFPR e tratados na política têm seu uso exclusivo para o desenvolvimento de atividades relacionados aos interesses da instituição, sendo essas de ensino, pesquisa, extensão, inovação e administrativas. É de obrigação da AGTIC ou da unidade que disponibilizou o recurso seu monitoramento, garantia de sua integridade, disponibilidade e segurança, assim como o suporte aos usuários. Qualquer software ou mecanismo cujo objetivo vise à obtenção de credenciais de acesso ou dados, causar danos ao patrimônio ou qualquer outro que possa ser caracterizado como fraude, sabotagem ou que possa

trazer risco à segurança das informações ali presentes, tem seu uso vedado. É proibida a utilização de qualquer ferramenta de compartilhamento ou divulgação de dados, arquivos e informações cuja classificação seja considerada confidencial a terceiros que não tenham autorização de acesso àqueles [39].

Equipamentos como computadores, tablets e smartphones cujo dono é a UFPR são todos compostos de forma padrão em relação ao hardware, sistema operacional e aplicativos pré-instalados, sendo essa padronização obrigação da unidade responsável pelo recurso. O acesso a qualquer um desses recursos deve ser sempre realizado de forma segura, utilizando senhas compatíveis com as políticas de segurança vigentes [39].

A AGTIC, caso o usuário deseje utilizar um dispositivo seu próprio para o acesso à rede da UFPR, poderá apenas prestar suporte em relação a orientações para as configurações necessárias para o uso da rede e seus sistemas. Caso seja detectado algum tipo de irregularidade no acesso à rede e a algum sistema, a Agência de Tecnologia da Informação e Comunicação tem o direito de bloquear esse acesso, de acordo com a Política de Uso de Recursos de TIC.

Todo dado institucional deve ser armazenado sempre levando em conta os recursos e ferramentas previamente aprovados pela AGTIC ou pela unidade responsável da UFPR. O compartilhamento dessas informações também deve seguir os procedimentos aprovados pelo órgão responsável, porém o compartilhamento de dados somente deve ocorrer quando houver uma autorização de seu autor. Fica proibido também manter dados institucionais em dispositivos desprotegidos, como unidades de armazenamento portáteis ou do próprio computador [39].

A Rede de Dados Institucional é uma rede privada cujo administrador é a AGTIC, e é constituída com o objetivo de permitir o tráfego de dados e o acesso à internet e aos sistemas. A rede pode ser acessada tanto com ou sem fio, e em cada ponto de acesso físico fica proibida a instalação de qualquer dispositivo de rede que seja do usuário final. Esses dispositivos podem ser hubs, switches, entre outros, podendo somente ocorrer sua implantação caso a Agência de Tecnologia de Informação e Comunicação da UFPR concorde. A Agência deve monitorar a rede sempre e, quando julgar necessário, pode adotar medidas como bloqueios, limitar a largura de banda e priorizar o tráfego para determinadas aplicações, de modo que as necessidades da Universidade sejam atendidas. [39]

É terminantemente proibido o uso da internet em sites que sejam considerados incompatíveis com as atividades exercidas na instituição, como por exemplo, sites que distribuem de forma ilegal softwares e arquivos, ou que ofereçam serviços ponto a ponto [39].

Conforme é descrito na Política de Uso de Recursos de TIC, todo usuário que esteja de acordo terá um e-mail "*@ufpr.br*". É obrigatório o uso desse e-mail em toda comunicação para assim poder garantir a segurança, integridade e autenticidade das comunicações realizadas, devendo utilizar o correio eletrônico que não seja da Instituição somente em comunicações inteiramente pessoais [39].

Em relação ao uso de recursos de impressão e digitalização, a Política de Uso de Recursos de TIC define normas claras para sua utilização. Somente será permitido o uso de recursos de impressão de digitalização para fins institucionais por colaboradores ativos, sempre respeitando as pautas de sustentabilidade, de forma a se evitar impressões desnecessárias e reduzir custos. Caso ocorra solicitação e essa seja aprovada, a AGTIC poderá fornecer equipamentos de impressão para um grupo de trabalho. Também é de responsabilidade da Agência o monitoramento do uso desses equipamentos.

Sobre o quesito de softwares, todo programa utilizado no âmbito da UFPR deverá possuir uma relação direta com as atividades desenvolvidas na universidade, e somente assim será permitido seu uso. O software deve respeitar todas as normas em relação à propriedade, licenciamento, cópia, reprodução e distribuição, seja ele comercial, livre ou desenvolvido internamente. É vedada a instalação de softwares não autorizados em equipamentos da instituição, sendo que a implantação de qualquer aplicativo em um equipamento próprio do usuário é de responsabilidade interina do mesmo [39].

Caso a AGTIC ou a unidade responsável pelo equipamento detecte algum tipo de irregularidade ou desacordo com a Política em relação a um software instalado em seu equipamento, esta tem o poder de bloquear, assim como desinstalar o software. Não é permitida a instalação de programas não autorizados pela Agência ou pela unidade responsável pelo equipamento, sendo que essas devem possuir uma lista de todos os softwares autorizados para consulta [39].

O armazenamento de softwares, tanto os desenvolvidos internamente pela UFPR como externos, devem ser aprovados pela AGTIC ou pela unidade responsável pelo servidor. Para que a aprovação seja realizada, serão avaliados os

impactos, riscos, conformidade com as normas e a viabilidade para que o software funcione de forma adequada [39].

Em relação a sites, somente após análise e aprovação pela AGTIC novos sites cujo domínio seja “ufpr.br” serão criados. Todo site terá ao menos um responsável, que terá por obrigações tratar de sua administração, manutenção e suporte, assim como manter o site atualizado. Qualquer tentativa de distribuir programas ou arquivos que possuam propriedade intelectual pelos sites é proibida, somente podendo ocorrer com a devida permissão de quem desenvolveu o recurso. Todo site desenvolvido deverá seguir norma, conforme descrito na Política de Uso de Recursos de TIC [39], para que exista um padrão em se tratando de “[...] metodologias de desenvolvimento, acessibilidade, identidade visual, a linguagem de programação, a documentação técnica, o manual do usuário, o controle de versões, o controle de acesso, as tratativas de dados pessoais e outras relacionadas à Segurança da Informação e Comunicação.”

Outros recursos de TIC que não são explicitamente tratados na política devem estar de acordo com as regras ali descritas, e é de responsabilidade da AGTIC elaborar, divulgar e manter uma lista contendo os recursos de TIC gerenciados pela mesma em local de fácil acesso. As unidades descentralizadas também têm essa obrigação [39].

Em se tratando do suporte desses recursos de TIC utilizados, esse deverá ser prestado pela unidade possuidora do recurso, a qual deve ter canais de suporte para atendimento aos seus usuários. Não será fornecido suporte a equipamentos do próprio usuário, somente aos que são de propriedade da UFPR.

É também vedado ao usuário abrir o equipamento para retirar peças ou cabos, alterar configurações previamente realizadas, exceto quando tal procedimento tenha sido orientado pelo suporte. Sempre que houver alguma dúvida em relação a algum recurso da UFPR, o usuário deve entrar em contato com a equipe técnica [39].

Caso ocorra perda, furto ou roubo, o usuário deve comunicar imediatamente à unidade gestora do recurso. Fica a cargo da unidade executar as medidas de prevenção para que não ocorra nenhum dano por terceiros e a reposição somente ocorrerá caso a unidade responsável pelo recurso aprove tal fato e exista a disponibilidade para substituição [39].

Na Política de Uso de Recursos de TIC também são definidas quais são as responsabilidades do usuário, das chefias, das autoridades responsáveis, dos

Gestores de Recursos, das equipes de suporte, dos gestores de contratos de serviços, das unidades de TIC descentralizadas e da AGTIC, e por fim, do Comitê de Tecnologia e Segurança da Informação e Comunicação. Com relação aos usuários, é dever deles sempre estarem informados sobre a política em questão, assim como suas possíveis atualizações. Também devem respeitar as normas correntes e utilizar esses recursos sempre em conformidade com as atividades institucionais. Caso seja detectada pelo usuário alguma irregularidade, é seu dever comunicar imediatamente ao gestor do recurso e à AGTIC ou unidade responsável, assim como se houver necessidade de algum suporte em relação ao recurso deve entrar em contato, formalmente, com a equipe técnica encarregada. Tendo em seu poder o equipamento, o usuário deve bloquear acessos não autorizados, assim como não deve gravar dados ou informações em dispositivos externos que não possuam o nível de segurança devido. Além disso, deve sempre manter seus dados o mais atualizado possível na unidade responsável [39].

Já as responsabilidades das chefias incluem que todos os seus servidores e usuários tenham conhecimento dessa Política e de demais normas de Segurança da Informação e Comunicação, assegurar que todos utilizem esses recursos de forma adequada e, quando necessário ou a pedido do Gestor de Recurso, autorizar, bloquear ou cancelar permissões e credenciais de acesso.

A Chefia também deve comunicar ao Gestor de Recurso e à AGTIC ou unidade descentralizada sobre possíveis problemas relacionados à Segurança da Informação e Comunicação [39].

Os Gestores de Recursos devem sempre garantir a disponibilidade, integridade, confidencialidade e a autenticidade das informações que forem disponibilizadas pelos recursos de TIC, assim como garantir que as equipes de suporte e atendimento estejam sempre cientes das atualizações sobre os processos para o acesso aos recursos. Além disso, é de responsabilidade dos Gestores, conforme é dito na Política “[...] prover controles que permitam o registro, monitoramento, rastreabilidade, prevenção e auditoria dos dados referentes à utilização dos recursos de TIC, principalmente aqueles críticos, zelando pelos prazos legais de manutenção dessas informações”. Devem também manter os registros da utilização dos recursos, assim como aplicar medidas cujo intuito é diminuir e/ou eliminar riscos de acessos indevidos aos Recursos de TIC. [39]

As equipes de atendimento e suporte devem sempre orientar os usuários quando estes tiverem dúvidas ou problemas com recursos de propriedade da UFPR, sempre sendo feito este contato através dos canais disponíveis, de acordo com a Política de Uso de Recursos de TIC.

Os responsáveis pelos contratos de serviços, também chamados de gestores, devem fazer com que a atual Política seja conhecida pelos prestadores de serviço, além de autorizar o acesso dos funcionários que estarão prestando o trabalho. Caso verifique que é necessário, pode alterar, bloquear ou cancelar o acesso durante a execução do serviço e, ao fim, deve cancelar o acesso previamente autorizado [39].

Toda unidade descentralizada de tecnologia de informação e comunicação deve garantir que suas regras internas estejam de acordo com a Política de Uso de Recursos de TIC e com as normas de segurança da UFPR [39].

A AGTIC, conforme a Política de Uso de Recursos de TIC, deve sempre manter a Política atualizada, divulgá-la para a comunidade da UFPR periodicamente utilizando os canais oficiais, possuir uma relação com todos os softwares homologados para a utilização em computadores da rede, assim como promover o desenvolvimento de projetos cujo objetivo é “melhoria contínua nos controles de acesso e utilização dos Recursos de TIC”.

Também presente na política [39] são as duas responsabilidades do Comitê de Tecnologia e Segurança da Informação e Comunicação, a saber: aprovar e promover a política no âmbito da UFPR e analisar e aprovar alterações na política.

Uma terceira Política existente na UFPR é a Política de Privacidade da UFPR. Esta tem por objetivo “ajudar os usuários a entender como os dados pessoais são coletados e utilizados pela UFPR”. Além das normas contidas nessa política, determinados sites e aplicativos podem apresentar termos adicionais devido às funcionalidades presentes e fornecidas. O primeiro item abordado é o direito à privacidade, o qual é garantido a todos e é protegido por lei. Conforme dito na Política [40], privacidade “[...] consiste na habilidade que este tem de controlar a exposição de informações sobre sua vida pessoal, sua intimidade, bem como a disponibilidade de dados sobre si mesmo, de retificar, ratificar ou apagar estes e de proteger a confidencialidade de suas comunicações, seu domicílio, sua imagem, honra e reputação perante terceiros”.

Seu segundo item aborda o propósito dos dados coletados, seu uso e armazenamento, e versa sobre as informações do usuário. Esses itens têm como finalidade, entre outras:

- Manter o cadastro dos usuários atualizados caso seja necessário haver comunicação;
- Informar sobre serviços, novidades e demais conteúdos relevantes da Universidade;
- Segurança do usuário e da UFPR;
- Cumprir ou contribuir com requisição ou ordem judicial;
- Auxiliar em melhorias tanto para o site como aplicativos da UFPR em relação a usabilidade, navegabilidade e interatividade, através de informações do meio utilizado (dispositivo, sistema operacional e navegador).

A base de dados formada pelos dados coletados utilizando o site e os aplicativos da UFPR são de propriedade e responsabilidade da Instituição, conforme está presente na Política de Privacidade. Toda informação que identifica os usuários não será vendida, comercializada ou alugada para terceiros, sendo que seu acesso e/ou compartilhamento somente pode ser feito mediante autorização do titular e quando o uso estiver dentro dos propósitos educacionais e acadêmicos.

Os dados somente poderão ser informados a outras instituições ligadas à UFPR, ao Ministério da Educação (MEC) e demais entidades cujo objetivo é promover a melhora da educação no país [40].

Somente profissionais internos autorizados pela Universidade Federal do Paraná podem acessar determinados dados, sempre respeitando os princípios presentes na política e, ainda, tal acesso somente será concedido caso o propósito seja condizente com a Universidade [40].

O usuário que entrou com suas informações em algum site ou aplicativo da UFPR tem total responsabilidade sobre a veracidade das mesmas, sendo sua responsabilidade corrigi-las ou atualizá-las, caso necessário. É garantido que esses dados coletados são armazenados em um servidor seguro próprio ou de terceiros, e todo servidor destinado a armazenamento de dados possui medidas de proteção

com “padrões de segurança e confidencialidade”, conforme descrito na Política de Privacidade.

Com relação ao uso de *cookies* – pequenos arquivos que guardam dados de navegação cujo objetivo é garantir o funcionamento correto dos sites e personalizar a navegação do utilizador – estes podem ser desativados caso o usuário deseje, porém, as utilizações desses serviços podem se tornar limitadas [40].

Os dados do usuário serão guardados pela UFPR enquanto este possuir algum vínculo com a Instituição. Uma vez finalizado esse vínculo, os dados serão armazenados por período determinado por lei, porém, caso esses dados façam parte do acervo histórico da UFPR, serão guardados de forma permanente. Caso deseje, o usuário ou seu responsável legal (no caso de usuário menor de idade) pode requerer que seus dados sejam excluídos, através de solicitação direta. Para que a exclusão ocorra deve ser levado em conta o prazo para que a exclusão possa ser feita, sendo este prazo iniciado a partir do momento que o usuário encerrar relações com a UFPR [40]

É salientado que todas as normas presentes na Política de Privacidade da UFPR podem ser alteradas a qualquer momento com o intuito de melhorá-las, e é dever do usuário estar ciente dessas mudanças quando vier a acessar sites e/ou fazer uso dos aplicativos da Instituição. A Política recomenda a leitura periódica do texto para que o usuário sempre esteja a par da situação.

Em relação a serviços prestados por empresas terceirizadas para algum tipo de processamento de dados utilizando os dados da UFPR, é dito na Política que “estas deverão, obrigatoriamente, respeitar as regras estipuladas nessa Política de Privacidade, nas políticas internas de Tecnologia da Informação e Comunicação e nas demais leis vigentes” [40].

Até o término desta pesquisa a Política de Privacidade da UFPR encontrava-se em processo de atualização, para atender ao modelo sugerido pelo Governo Federal [48].

A Agência de Tecnologia da Informação e Comunicação da UFPR também já implementou várias mudanças em relação aos princípios de proteção de dados da nova Lei Geral de Proteção de Dados. Com relação à finalidade dos dados coletados, a AGTIC já está orientando processos que coletem dados pessoais e dados sensíveis a declararem o propósito daqueles dados, assim como solicitar que participantes do estudo estejam de acordo com os experimentos em questão.

Também foi adotada a medida de informar o propósito de cada dado requerido em dois documentos publicados no ano de 2020: o Edital da PRAE para empréstimo de notebooks a alunos e no edital para o Vestibular da UFPR 2021 [41].

Sobre o princípio da segurança, a Agência de Tecnologia da Informação e Comunicação da Universidade elaborou as três políticas citadas previamente, a Política de Acesso, a Política de Uso de Recursos de TIC e a Política de Privacidade. Para sua efetivação, basta apenas a aprovação pelo Comitê de Tecnologia e Segurança da Informação e Comunicação, e pelo Conselho de Planejamento e Administração (COPLAD). Também foram inclusas nas ações de conscientização sobre segurança, informações e recomendações sobre o tratamento de dados pessoais e sensíveis. Na primeira semana de dezembro de 2020 a Instituição adquiriu um sistema antivírus e, até o término desta pesquisa, a implantação encontrava-se em fase experimental dentro da AGTIC para que, em janeiro de 2021, pudesse ser iniciada sua implantação em toda a Instituição [41] [48].

Atendendo ao princípio da prevenção e também ao princípio anterior da segurança foi implantando em 2019 um novo Firewall, cujo argumento de compra foi baseado na LGPD. Em novembro de 2020 todas as funcionalidades do Firewall foram ativadas e, até o término desta pesquisa, estava em tramitação um processo para aquisição de um novo backup comercial, cuja confiança é maior em relação ao sistema em uso.

Em se tratando dos princípios de adequação, necessidade, livre acesso, transparência e não discriminação, ainda não foram definidas medidas concretas sobre esses pontos da lei. Porém, conforme já mencionado, foi contratada empresa especializada em análise de ambiente e implantação da LGPD, com início da prestação do serviço à UFPR previsto para 2020. Já em relação à qualidade dos dados, a AGTIC entende a necessidade de atender a esse princípio, porém, devido a barreiras, entre elas políticas, há uma grande dificuldade em relação a esse fundamento da Lei. Algo que também complica a aplicação de medidas para ficar de acordo é que existem informações presentes em várias bases de dados, e muitas vezes existem dados duplicados nessas bases [41].

O último princípio abordado na Lei, o de responsabilização e prestação de contas, é abordado através da criação do comitê para planejamento de implantação da LGPD e da nomeação do DPO da Instituição, conforme citado previamente.

O comitê para planejamento de implantação da LGPD avaliou que não havia embasamento suficiente, e decidiu que uma empresa especializada em análise de ambiente e implantação das políticas da LGPD deveria ser contratada. Utilizar uma instituição externa para realizar a adaptação em toda a UFPR não funcionaria, uma vez que o tamanho da Universidade é muito grande, portanto foi definido que o próprio comitê para planejamento de implantação da LGPD compreenderia as necessidades e normas, e a comissão realizaria as mudanças necessárias. O trabalho da instituição terceirizada consistirá em realizar o diagnóstico da Universidade e ensinar os primeiros passos ao comitê, para que seja possível a realização destas mudanças posterioemente pela própria comissão [1].

Devido à urgência de realizar esse trabalho o comitê para planejamento de implantação da LGPD, antes mesmo das primeiras reuniões com essa instituição terceirizada, já realizou reuniões para o estudo de como será executada essa implantação, além de levantamento prévio a respeito das fontes de dados pessoais. Processos que se encontravam frágeis já passaram por definições com as partes envolvidas [48].

O principal produto a ser entregue por essa empresa contratada é um documento no qual serão informadas todas as vulnerabilidades dos dados presentes na UFPR e quais ações devem ser tomadas para a neutralização de tais fragilidades [1].

Questões ainda pendentes em relação à LGPD incluem retrabalhar o acesso e a anonimização dos dados, e espera-se que, uma vez concluído o serviço da empresa especializada em implantação das regras da nova Lei, possam ser realizadas as mudanças necessárias com relação a esse tópico [41].

Em seguida, o último capítulo deste trabalho apresenta as conclusões e recomendações decorrentes da pesquisa realizada.

5 CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Neste capítulo serão apresentadas as principais conclusões do presente trabalho e a recomendação para estudos futuros na área.

5.1 CONCLUSÕES

A pesquisa realizada para este trabalho de conclusão de curso evidenciou as dificuldades iniciais no processo de implementação da LGPD, obstáculos que se colocam não apenas na UFPR, mas para todas as organizações que armazenam e tratam dados como parte de sua função e produção. Sendo assim, supõe-se que a produção acadêmica e científica sobre o tema deve continuar em crescimento, refletindo as dificuldades encontradas e também as soluções que serão implementadas.

Considerando as informações apresentadas e a Lei Geral de Proteção de Dados em vigor desde a data de 18 de setembro de 2020, entende-se que deve haver, entre o curto e o médio prazo, uma grande mudança nos sistemas de software nas instituições públicas e privadas. Essa mudança vem acompanhada de uma transformação no pensamento de programadores, analistas, engenheiros e outras pessoas do ramo de desenvolvimento de software ao produzir, adaptar ou até mesmo realizar uma simples mudança em um determinado software. Com a LGPD, a conformidade à Lei passa a ser um requisito não funcional obrigatório.

Neste processo de adequação o papel dos gestores organizacionais (chefias, coordenações, diretorias e gerências médias) será fundamental, convocando e dirigindo equipes de trabalho que, obrigatoriamente, deverão apresentar um caráter multidisciplinar. Pode-se dizer – com razoável nível de segurança – que o profissional formado pela Ciência da Computação terá lugar garantido neste processo, sendo o responsável por estabelecer uma ponte entre o fator humano e a eficiência dos softwares que farão a gestão e armazenamento dos dados. As múltiplas camadas de segurança necessárias, por exemplo, apontam que o profissional de T.I. precisará prever categorias diferentes de usuários e níveis de acesso, garantindo simultaneamente a usabilidade dos programas e ferramentas a todos os envolvidos.

Para que ocorra sucesso na implementação e, posteriormente, implantação das novas políticas presentes na LGPD, é necessário que aconteçam adaptações para deixar todos os funcionários de instituições públicas e privadas cientes da mesma. Conforme mencionado anteriormente, essa mudança que a nova Lei traz não afeta somente o setor de T.I. das instituições privadas ou públicas, mas sim todo o negócio, devido às novas regras e modificações que deverão ser feitas em outras áreas, além da técnica, confirmando a multidisciplinariedade da LGPD.

Deve-se fazer um levantamento dos dados utilizados pelas instituições públicas e privadas, verificar se existem dados sensíveis e, caso existam, deve-se averiguar sua finalidade, se realmente são necessários para aquele contexto. A conscientização da comunidade e dos colaboradores é o primeiro passo para o estabelecimento mais profundo da mudança da cultura organizacional, necessária na instituição pública ou privada em que as normas estão sendo aplicadas. Esta mudança ocorre através do reconhecimento de passos iniciais, como a organização de documentos tanto físicos como digitais, uma pequena mudança que pode trazer benefícios a todos. Estas são apenas algumas das etapas necessárias para que o início da implementação das regras contidas na LGPD possa ser realizado. Instituições públicas e privadas que estão em concordância com a Lei N° 13.709/2018 oferecerão garantias adicionais aos seus clientes e usuários, e a segurança de que qualquer dado ou informação compartilhada estará protegida.

Caso ocorra algum tipo de problema com relação aos dados pessoais tratados por uma instituição pública ou privada observa-se que não é apenas o setor no qual ocorreu o problema que terá contratempos, ou seja, não é apenas o operador ou o controlador que serão os culpados, mas sim toda a instituição que terá responsabilidade, comprovando a abrangência operacional e legal da Lei N° 13.709/2018. Apesar das punições decorrentes da LGPD serem somente aplicadas a partir da data de 1° de agosto de 2021, a Lei já está em vigor, e os softwares que não estão conforme as novas regras devem ser corrigidos o mais rápido possível.

A questão tratada pela LGPD, a regulamentação e a definição de condições para o tratamento de dados pessoais por instituições públicas e privadas, sempre foi necessária, independentemente de haver uma lei específica para isso ou não. Toda instituição pública ou privada deve estar ciente das novas regras impostas pela legislação, pois houve significativo tempo decorrido desde a aprovação da nova Lei para que as instituições pudessem estudar seu texto e realizar as adequações.

Em se tratando do estudo de caso da UFPR, é possível usar como exemplo os sistemas de softwares que gerenciam as bases de dados dos alunos, professores e funcionários das Universidades. De acordo com dados de 2020, a UFPR é composta por 2.590 docentes, 3.450 técnicos administrativos e 38.242 alunos. Todos estes discentes tiveram que preencher vários dados quando fizeram a inscrição para o vestibular, dados estes pessoais e em muitos casos sensíveis. É necessário que exista toda a proteção adequada a esses dados do candidato. Deve haver uma

cooperação entre as áreas meio e as áreas fim da Universidade de modo que todos os documentos, processos e sistemas sejam padronizados.

Através da Política de Segurança da Informação da UFPR (PSI/UFPR), a Universidade Federal do Paraná possui uma relação de regras muito completa, na qual pode-se perceber várias semelhanças com diversos pontos da LGPD. Mesmo sendo uma Resolução publicada no ano de 2014, a PSI/UFPR se mantém muito atual, pois, por exemplo, tanto na Lei como na Resolução existe a figura de um profissional cuja função é similar à do Encarregado de Proteção de Dados (DPO - *Data Protection Officer*), responsável pela segurança dos dados.

A UFPR já instituiu o comitê para planejamento da implantação da LGPD e o Encarregado de Proteção de Dados da Universidade pelas Portarias N° 1130/Reitoria e N° 1393/Reitoria, respectivamente, e com essas ações efetivamente iniciou seu processo para se adequar à nova Lei.

O FAQ (*Frequently Asked Questions*) produzido pelo DPO da Universidade, o Termo de Privacidade do Vestibular e o Edital da PRAE para repasse de *notebooks* a alunos em vulnerabilidade, são documentos que foram escritos contendo todas as informações conforme a Lei orienta, e demonstram que a UFPR já está ciente do que a LGPD significa, trabalhando para que toda a Instituição fique em concordância com a nova norma. A contratação de uma empresa especializada para ajudar na adaptação da Instituição é outra ação que comprova que não há tempo a perder, e que as alterações devem ser realizadas o quanto antes.

As novas políticas definidas pela Agência de Tecnologia da Informação e Comunicação (AGTIC), juntamente com o diagnóstico que será realizado pela empresa externa, caracterizam o movimento da Universidade para se adequar às regras estabelecidas pela LGPD.

Também dentro da AGTIC, já foi iniciada uma mudança de cultura com alguns de seus colaboradores, uma vez que os estudos para adquirir conhecimentos sobre a Lei N° 13.709/2018 vem ocorrendo desde 2018. Conforme expresso pela própria gerência da AGTIC, em determinados processos já foram tomadas decisões, de modo que seus responsáveis já estão instruídos sobre o procedimento para obter maior segurança e informação em relação à LGPD. A Agência também tem ciência da necessidade de envolvimento de todos os membros da comunidade da UFPR, buscando a mudança da cultura organizacional no tratamento de dados pessoais e dados sensíveis. Reconhece-se que, possivelmente, haverão dificuldades para

operar a mudança de forma completa na comunidade, mas também-se compreende-se internamente que é um processo necessário e irreversível no longo prazo.

É necessário que todos os envolvidos (discentes, docentes, servidores técnico-administrativos, terceirizados) com a Universidade Federal do Paraná conheçam a LGPD e as Políticas da UFPR com relação a proteção de dados. Conforme consta nas Políticas da Universidade, é dever da AGTIC informar a todos da comunidade da UFPR a respeito das novas normas presentes na Política de Controle de Acesso e na Política de Uso de Recursos de TIC. Alunos, professores e servidores técnico-administrativos que entrarem na Instituição devem saber que ela está comprometida com a Lei Geral de Proteção de Dados e que seus dados estão seguros, pois a Universidade está comprometida com a Lei.

Conforme já abordado no texto, a principal barreira a ser vencida para que a Lei N° 13.709/2018 seja implantada com sucesso é a mudança de cultura com relação às pessoas envolvidas no processo. Somente com essa mudança de cultura, a aplicação das regras contidas na Política de Segurança da Informação será processada de forma efetiva. É importante que passos iniciais na mudança envolvam pleno acesso à informação da LGPD, bem como capacitações junto aos colaboradores da Universidade para que incidentes envolvendo vazamento ou extravio de dados não venham a ocorrer. Estes passos iniciais são importantes para o início da conscientização a respeito de como cada colaborador deve considerar o conceito de “dado”, e essa própria capacitação é considerada uma nova camada de segurança.

A Instituição mobiliza-se para que sejam realizados os ajustes necessários para a LGPD, e a decisão de contratar somente instituições privadas que estejam totalmente adequadas à Lei para qualquer tipo de prestação de serviço demonstra que a UFPR está ciente de que todos devem respeitar as novas regras. Por ser uma Instituição Pública, a Universidade não contrata empresas que não estejam de acordo, não só com a LGPD, como com todas as Leis.

Uma vez que o diagnóstico da Universidade seja entregue ao comitê para planejamento de implementação da LGPD e à AGTIC, estes terão a missão de adaptar todos os sistemas de tecnologia e organizacionais da Universidade, assim como todos os dados e informações presentes nos bancos de dados devem passar por vistoria. O comitê para planejamento de implantação da LGPD e a AGTIC deve adotar medidas de segurança, técnicas e administrativas, de forma que todos os

dados pessoais da Instituição não sofram acessos não autorizados e/ou qualquer espécie de tratamento indevido que possa vir a causar danos às informações.

Os futuros profissionais do curso de Ciência da Computação terão a responsabilidade de realizar as novas adequações que forem necessárias para a correta implantação da Lei N° 13.709/2018, conforme já citado no texto em relação às áreas de T.I. No curso de Bacharelado em Ciência da Computação da UFPR, a Lei Geral de Proteção de Dados é abordada dentro da disciplina de Segurança Computacional. Também ocorrem seminários e outras abordagens pontuais, transversais às disciplinas, sobre a LGPD, que deve ocupar espaço cada vez maior nos currículos de cursos ligados às Tecnologias e Ciências da informação e Computação.

Os estudante atuais dos cursos de Ciência da Computação provavelmente terão papel fundamental e extenso em um contexto de trabalho que será progressivamente mais preocupado com o armazenamento seguro de dados, desenvolvendo maneiras mais efetivas para garantir a interface adequada entre usuários e dados protegidos. Portanto, desponta a necessidade de explorar também de forma mais aprofundada o tipo de formação inicial que este profissional recebe, identificando *gaps* no currículo básico e sugerindo novas opções formativas que complementem a formação para atuação nesta área de trabalho.

A formação básica pode ser aperfeiçoada, por exemplo, com o conhecimento de normas e padronizações aplicados nas organizações. Embora a ISO 27001 tenha sido explorada em mais detalhes neste trabalho, ficou também evidente que ela não é parâmetro único de qualidade, ou referência de boas práticas definitiva para a proteção e tratamento de dados pessoais e sensíveis. Sendo assim, sobressai a possibilidade de estudar mais detidamente recursos como aqueles oferecidos pela comunidade OWASP e pelo NIST, possibilitando a ampliação do escopo de soluções possíveis nos problemas de implementação da LGPD.

É importante a inserção de conteúdos da LGPD quando os cursos tratam de dados pessoais e sensíveis em projetos de pesquisa, de modo que esses estudos estejam de acordo com a Lei e seus pesquisadores saibam como aplicar as normas em seus futuros projetos.

Em relação aos servidores e professores, também é necessária essa comunicação para que todos saibam sobre a Lei, para que possam fazer o uso de suas normas em seu trabalho quando necessário.

Caso não ocorram ações de treinamento, de capacitação para a LGPD com os discentes, docentes e servidores técnico-administrativos, a rotina de uso da nova Lei ficará restrita à AGTIC, ao comitê para planejamento de implantação da LGPD e ao DPO. A delimitação destes saberes e práticas apenas às áreas e comitês específicos denotará a falta da devida capilaridade do conhecimento, impedindo ações necessárias que requerem o engajamento de toda comunidade acadêmica e dificultando a mudança da cultura organizacional.

Todos os documentos elaborados pelos setores e órgãos da Universidade deverão estar conforme a Lei decreta e, para que isso ocorra, serão necessários treinamentos em todos os setores e áreas administrativas da Universidade.

A AGTIC e o comitê para planejamento de implantação da LGPD da Universidade têm a obrigação de divulgar as informações sobre a nova Lei a todos da comunidade acadêmica como garantia de um direito do cidadão. Neste sentido, a realização de palestras, seminários e outros eventos de divulgação são ferramentas assertivas à disposição da Agência para divulgar a LGPD e provocar a discussão da comunidade de professores, técnicos e discentes.

A implantação da Lei N° 13.709/2018 será muito trabalhosa para a Agência de Tecnologia da Informação e Comunicação, pois deverá realizar a atualização em todos os seus sistemas. Porém, compreende-se que o esforço é necessário e coerente, pois a nova Lei Geral de Proteção de Dados veio para fazer parte do desenvolvimento tecnológico do país, e confere maior transparência no uso dos dados dos titulares tanto nas instituições públicas como privadas.

Esta pesquisa também deixou clara a importância do envolvimento abrangente de todos os participantes de uma instituição para a implementação adequada e efetiva da LGPD, já que apenas um usuário descuidado pode ser suficiente para comprometer toda uma estrutura complexa de dados. Embora a implementação de camadas de segurança seja uma tarefa eminentemente técnica, é o fator humano que complementará e garantirá o funcionamento seguro de uma rede de dados, evitando vazamentos, extravio ou deslocamento equivocado de informações.

Finalmente, ficou evidente que o fator humano, o comportamento individual, deve ser considerado na implementação de qualquer estudo sobre a LGPD, tendo em vista a necessidade de formar, capacitar e conscientizar todas as pessoas que participam ou acessam redes de dados na instituição. A mudança individual na aquisição, armazenamento e tratamento de dados é o passo mais importante para

criar uma cultura coletiva de proteção e segurança de informações, tratando cada pessoa como um agente ou elo em uma cadeia complexa que contribuirá para a preservação dos conceitos da LGPD.

5.2 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

- Ampliação das pesquisas sobre a aplicação da LGPD em Universidade Públicas e Privadas;
- Estudos sobre a utilização das Guias Operacionais para adequação à LGPD disponibilizados pelo Governo Federal;
- Explorar recursos da comunidade OWASP e do NIST na implantação da LGPD;
- Abordagem mais incisiva da LGPD dentro dos cursos de Ciência da Computação;
- Elaboração de seminários e outras atividades de capacitação para a implantação da LGPD.

REFERÊNCIAS

[1] PEREIRA, V. A. A AGTIC e a LGPD. Curitiba. 9 nov. 2020. Informação verbal.

[2] BRASIL. Lei n° 13.709, de 8 de julho de 2018. Institui a Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 5 de out. 2020.

[3] TIMOCHENCO, Longinus. Como a ISO 27001 pode ajudar a sua empresa com a LGPD. **Infra News Telecom**, 2019. Disponível em: https://www.infranewstelecom.com.br/como-a-iso-27001-pode-ajudar-a-sua-empresa-com-a-lgpd/. Acesso em: 12 dez. 2020.

[4] LGPD: Qual o impacto da LGPD no setor de TI? **Agasus**, 2020. Disponível em: https://agasus.com.br/gestao-de-ti/qual-o-impacto-da-lgpd-no-setor-de-ti/. Acesso em: 5 out. 2020.

[5] A Autoridade Nacional de Proteção de Dados. É claro que, antes de fiscalizar e penalizar um ente, a ANPD orientará sobre como aplicar a lei? **Serpro**, 2019. Disponível em: https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd. Acesso em: 5 out. 2020.

[6] SCHREIER, J. **Blood, Sweat and Pixels**: The triumphant, Turbulent Stories Behind How Video Games Are Made. New York: Harper Paperbacks, 2017.

[7] PRESSMAN, Roger S. **Engenharia de Software**: Uma Abordagem Profissional. Porto Alegre: AMGH, 2011.

[8] SOMMERVILLE, I. **Engenharia de Software**. São Paulo: Pearson Prentice Hall, 2011.

[9] WAZLAWICK, Raul S. **Engenharia de Software**: Conceitos e Práticas. Rio de Janeiro: Elsevier, 2013.

[10] GUIMARÃES, G. Reunião LGPD Órgão Público [Mensagem Pessoal]. Mensagem recebida por: fabio.mello1997@gmail.com. 27 jul. 2020.

[11] TERMO DE PRIVACIDADE DO PORTAL DO CANDIDATO VESTIBULAR UFPR 2020/2021. **Universidade Federal do Paraná**, 2020. Disponível em: http://portal.nc.ufpr.br/documentos/termo_privacidade/Termo_de_privacidade_PS_UFPR_2021.pdf. Acesso em: 7 nov. 2020.

[12] SOMADOSSI, Henrique. O que muda com a Lei Geral de Proteção de Dados (LGPD). **Migalhas**, 2018. Disponível em: https://www.migalhas.com.br/depeso/286235/o-que-muda-com-a-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 26 set. 2019.

[13] DURBANO, Vinicius. LGPD: tudo o que você precisa saber sobre a lei de proteção de dados. **Ecoit**, 2018. Disponível em: https://ecoit.com.br/lgpd/. Acesso em: 26 set. 2019.

[14] 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais, mostra pesquisa da Serasa Experian. **Serasa Experian**, 2019. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian. Acesso em: 5 out. 2020.

[15] Pesquisa indica baixa adesão à Lei Geral de Proteção de Dados. **Revista Exame**, 2020. Disponível em: https://exame.com/tecnologia/pesquisa-indica-baixa-adesao-a-lei-geral-de-protecao-de-dados/. Acesso em: 15 nov. 2020.

[16] O que é a ISO 27001? **Advisera**, 2019 https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/. Acesso em: 5 out. 2020.

[17] KOSUTIC, Dejan. Lista de verificação para implementação da ISO 27001. **Advisera** 2020. Disponível em: https://advisera.com/27001academy/pt-br/knowledgebase/lista-de-verificacao-para-implementacao-da-iso-27001/. Acesso em: 5 out. 2020.

[18] Proteja seus ativos de informação. **Lloyd's Register**, 2019. Disponível em: https://www.lr.org/pt-br/iso-27001/. Acesso em: 5 out. 2020.

[19] O que são dados Anonimizados, segundo a LGPD. **Serpro**, 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd. Acesso em: 30 maio 2020.

[20] Quem é o DPO? Conheça o Novo Guardião dos Dados Pessoais. **LGPD Brasil**, 2020. Disponível em: https://www.lgpdbrasil.com.br/quem-e-o-dpo-conheca-o-novo-guardiao-dos-dados-pessoais-2/. Acesso em: 5 out. 2020.

[21]. MEDEIROS, Henrique. Quem é o DPO, profissional que ganhará espaço nas empresas com a LGPD. **Mobile Time**, 2018. Disponível em: https://www.mobiletime.com.br/noticias/08/11/2018/dpo-o-profissional-que-ganhara-espaco-nas-empresas-com-a-lgpd/. Acesso em: 5 out. 2020.

[22] BEDFORD, Russell. Por que é Urgente a Real Efetivação da ANPD Neste Ano de 2020? **Russell Bedford**, 2020. Disponível em: https://russellbedford.com.br/noticias/por-que-e-urgente-a-criacao-da-anpd-neste-ano-de-2020/. Acesso em: 5 out. 2020.

[23] LGPD: proteção de dados e papel do professional de TI. **Blog da CCM**, 2018. Disponível em: https://blog.ccmtecnologia.com.br/post/lgpd-protecao-de-dados-e-o-papel-do-profissional-de-ti. Acesso em: 5 out. 2020.

[24] O que significa "privacy by design" e qual a relação com a LGPD. **Ostec**, 2019. Disponível em: https://ostec.blog/geral/privacy-by-design. Acesso em: 5 out. 2020.

[25] FARIA, William Rodrigues de. LGPD e GDPR: 7 princípios que a TI deve colocar em prática. **CIO**, 2019. Disponível em: https://cio.com.br/gestao/lgpd-e-gdpr-7-dicas-para-coloca-las-em-pratica-em-ti/. Acesso em: 5 out. 2020.

[26] Lei de Proteção de Dados chega às escolas: saiba como se preparar. **Escolas Exponenciais**, 2019. Disponível em: https://escolasexponenciais.com.br/desafios-contemporaneos/lei-de-protecao-de-dados/. Acesso em: 5 out. 2020.

[27] WIK, Roberto. Lei Geral de Proteção de Dados (LGPD): por onde começar? **Computerworld**, 2019. Disponível em: https://computerworld.com.br/2019/02/04/lei-geral-de-protecao-de-dados-lgpd-por-onde-comecar/. Acesso em: 5 out. 2020.

[28] Privacy by Design e by Default: entenda a diferença. **Privacy Tech**, 2019. Disponível em: https://privacytech.com.br/noticias/privacy-by-design-e-by-default-entenda-a-diferenca,322343.jhtml. Acesso em: 5 out. 2020.

[29] LIMA, Ramalho. Bolsonaro sanciona LGPD que entra em vigor hoje (18). **Tecmundo**, 2020. Disponível em: https://www.tecmundo.com.br/seguranca/189099-sancionada-bolsonaro-lgpd-entra-vigor-18.htm?f. Acesso em: 25 set. 2020.

[30] Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD). **Governo Federal**, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 22 out. 2020.

[31] ISO 27001 – Sistema de Gestão de Segurança da Informação. **INTEGRITY**, 2020. Disponível em: https://www.27001.pt/. Acesso em: 22 out. 2020.

[32] Brasil. Lei n° 12.965, de 32 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 29 out. 2020.

[33] REDAÇÃO. Senado confirma primeira diretoria da Autoridade Nacional de Proteção de Dados. **Senado Notícias**, 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados. Acesso em: 3 nov. 2020.

[34] SAID, Flávia. Senado aprova primeiro conselho diretor da ANPD, com maioria de origem militar. **Congresso em Foco**, 2020. Disponível em: https://congressoemfoco.uol.com.br/legislativo/ao-vivo-senado-vota-indicacao-de-autoridades-para-as-agencias-reguladoras/. Acesso em: 3 nov. 2020.

[35] Agência de Tecnologia da Informação e Comunicação. **AGTIC**, 2020. Disponível em: https://www.agtic.ufpr.br/portal/a-agtic/. Acesso em: 30 out. 2020.

[36] Resolução N° 45/19-COPLAD. **Universidade Federal do Paraná**, 2019. Disponível em: http://www.soc.ufpr.br/portal/wp-content/uploads/2019/11/coplad-45.19.pdf. Acesso em: 30 out. 2020.

[37] MELO, Leonardo. LGPD na UFPR [Mensagem Pessoal]. Mensagem recebida por: fabio.mello1997@gmail.com. 7 nov. 2020.

[38] UFPR. Política de Controle de Acesso. Curitiba, 2020.

[39] UFPR. Política de Uso de Recursos de TIC. Curitiba, 2020.

[40] UFPR. Política de Privacidade da UFPR. Curitiba, 2020.

[41] PEREIRA, Valmir Antunes. Princípios da LGPD na AGTIC [Mensagem Pessoal]. Mensagem recebida por: fabio.mello1997@hotmail.com. 12 nov. 2020.

[42] Resolução N° 21/14-COPLAD. **Universidade Federal do Paraná**, 2014. Disponível em: http://www.soc.ufpr.br/portal/wp-content/uploads/2016/07/resolucao_coplad_17112014-959.pdf. Acesso em: 4 jul. 2020.

[43] Publicada, com vetos, lei que cria a Autoridade Nacional de Proteção de Dados. **Consultor Jurídico**, 2019. Disponível em: https://www.conjur.com.br/2019-jul-09/publicada-lei-cria-autoridade-nacional-protecao-dados. Acesso em: 10 set. 2020.

[44] SC, Tech. Lei que cria a Agência Nacional de Proteção de Dados é publicada. **NSC Total**, 2019. Disponível em: https://www.nsctotal.com.br/noticias/lei-que-cria-a-agencia-nacional-de-protecao-de-dados-e-publicada. Acesso em: 10 set. 2020.

[45] WHITTAKER, Zack. Hackers stole customer credit cards in Newegg data breach. **Techcrunch**, 2018. Disponível em: https://techcrunch.com/2018/09/19/newegg-credit-card-data-breach/. Acesso em: 20 maio 2019.

[46] WHITTAKER, Zack. Indian state government leaks thousands of Aadhaar numbers. **Techcrunch**, 2019. Disponível em: https://techcrunch.com/2019/01/31/aadhaar-data-leak/. Acesso em: 20 maio 2019.

[47] VALENTE, Jonas. Entenda o que muda com a Lei Geral de Proteção de Dados. **Agência Brasil**, 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/entenda-o-que-muda-com-a-lei-geral-de-protecao-de-dados#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20entrou%20em%20vigor,e%20tratamento%20de%20informa%C3%A7%C3%B5es%20pessoais. Acesso em: 14 dez. 2020.

[48] PEREIRA, V. A. A AGTIC e a LGPD. Curitiba. 14 dez. 2020. Informação verbal.

[49] MONTEIRO, Luis Felipe Salin. INSTRUÇÃO NORMATIVA SGD/ME Nº 117, DE 19 DE NOVEMBRO DE 2020. **Diário Oficial da União**, 2020. Disponível

em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596. Acesso em: 14 dez. 2020.

[50] FINELLI, Alexandre. LGPD exigirá esforço multidisciplinar. **Security Report**, 2018. Disponível em: https://www.securityreport.com.br/destaques/lgpd-exigira-esforco-multidisciplinar/. Acesso em: 14 dez. 2020.

[51] Guias Operacionais para adequação à LGPD. **Governo Digital**, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd. Acesso em: 14 dez. 2020.

[52] ANDRADE, Vitor Morais, KIM, Stella He Jin. Possuir a certificação ISO/IEC 27001:2013 significa estar Compliance com a LGPD? E quais as expectativas para a ISO/IEC 27701:2019? **Migalhas**, 2019. Disponível em: https://migalhas.uol.com.br/depeso/309466/possuir-a-certificacao-iso-iec-27001-2013-significa-estar-compliance-com-a-lgpd--e-quais-as-expectativas-para-a-iso-iec-27701-2019. Acesso em: 15 dez. 2020.

[53] RODRIGUES, Rafael. O que é ISO 27701? **ProMove Soluções**, 2020. Disponível em: https://promovesolucoes.com/o-que-e-iso-27701/. Acesso em: 15 dez. 2020.

[54] OWASP. Disponível em: https://owasp.org/. Acesso em: 15 dez. 2020.

[55] NIST divulga recomendação para gerenciamento de riscos de privacidade. **TI INSIDE**, 2020. Disponível em: https://tiinside.com.br/17/01/2020/nist-divulga-recomendacao-para-gerenciamento-de-riscos-de-privacidade/. Acesso em: 15 dez. 2020.

[56] LGPD exigirá mudança na cultura empresarial. **Infra TI**, 2019. Disponível em: https://infrati.com.br/lgpd-exigira-mudanca-na-cultura-empresarial/. Acesso em: 15 dez. 2020.

[57] Quais são os desafios que a LGPD traz para o time de TI. **Algar Tech**, 2020. Disponível em: https://algartech.com/pt/blog/desafios-e-impactos-da-lgpd-na-ti/. Acesso em: 15 dez. 2020.

[58] ZEFERINO, Denis. LGPD para profissionais de TI: importância da legislação. **Certifiquei**, 2020. Disponível em: https://www.certifiquei.com.br/lgpd-profissionais-ti/. Acesso em: 15 dez. 2020.

[59] Serpro é protagonista em capacitação sobre LGPD no país. **Serpro**, 2020. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2020/serpro-protagonista-capacitacoes-protecao-lgpd. Acesso em: 16 dez. 2020.