ESTUDO SOBRE A ADEQUAÇÃO DAS EMPRESAS BRASILEIRAS ÀS NOVAS DIRETRIZES DA SEGURANÇA DE DADOS DA LGPD

Marcio Aurélio de Souza Fernandes, Edna Dias Canedo, Rodrigo Marques dos Santos, Fábio Lúcio Lopes de Mendonça, Daniel Alves da Silva e Rafael Timóteo de Sousa Jr
Universidade de Brasília – UNB, Campus Universitário Darcy Ribeiro, Brasília – DF, CEP 70910-900, Brasil

RESUMO

Com a entrada em vigor da LGPD, em 2020, houve um aumento na fiscalização por parte dos órgãos competentes, e parte das organizações estão com grande dificuldade em se adequar à legislação. Diante do exposto, o trabalho foi realizado para avaliar o nível de conhecimento dos profissionais das áreas de tecnologia que atuam em corporações públicas ou privadas. O trabalho foi dividido em duas etapas de execução, a saber: 1) uma análise das legislações sobre a privacidade de dados; e 2) a condução de um *survey* com 43 profissionais de tecnologia que atuam em organizações públicas e privadas. O *survey* contém 21 questões que abrangem legislação e tecnologia. Os resultados demonstram que, mesmo após a LGPD entrar em vigor, 10% dos profissionais de ICT não conhecem os princípios da Lei. Em relação à forma de armazenamento seguro, 45% dos profissionais de ICT afirmaram não ter conhecimento de como suas organizações realizam o armazenamento dos dados dos usuários ou o compartilhamento desses dados. 25% dos profissionais de ICT afirmaram que estão cientes que seus dados podem ser compartilhados pelas organizações.

PALAVRAS-CHAVE

Proteção de Dados, Segurança da Informação, Privacidade de Dados, LGPD, Conformidade e Adequação

1. INTRODUÇÃO

Em meio à crescente utilização da internet para atividades rotineiras, como comércios eletrônicos (e-commerce), transações bancárias online, criações de novas mídias sociais, que cada vez mais expõem os dados pessoais dos seus utilizadores, os criminosos voltaram seus ataques para esses usuários. A Lei Geral de Proteção de dados – LGPD (REPÚBLICA, P., 2018) foi elaborada com o objetivo de controlar e fortalecer os direitos dos cidadãos sobre suas informações pessoais e sua privacidade.

A proteção de dados ganhou ênfase nos últimos anos com o aumento de ataques e vazamentos de dados, deixando de ser um problema apenas de corporações bancárias ou agencias financeiras, tornando-se um problema para todos os ramos de atividades. A prática dessas empresas em ter, em seu banco de dados, os cadastros de usuários e clientes faz com que criminosos cibernéticos vislumbrem nesse contexto a grande chance de aplicar golpes, fraudes, sequestro de dados, etc. Dificilmente a implantação de novas tecnologias seguem as recomendações das boas práticas em gestão da informação, tais como as normas da *International Organization for Standardization* (ISO)(ISO-16363-2012), e o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil), os quais visam descrever os requisitos mínimos e os desejáveis para garantir a cadeia de custódia documental e proteção dos dados do usuário.

Para gerar o resultado esperado, foi utilizada a metodologia mista, ou seja, elaborando um questionário para avaliação do conhecimento das pessoas envolvidas no processo de desenvolvimento de ferramentas/soluções e/ou usuários, sobre a temática da privacidade de dados (metodologia quantitativa). O questionário apresenta 21 questões referentes à LGPD e à segurança da informação, com intuito de colher informações sobre o nível de conhecimento dos profissionais que atuam diretamente com sistemas e com a legislação.

2. GDPR E LGPD

A *General Data Protection Regulation* – GDPR (REGULATION , 2018), assim como várias outras leis e regulamentos, surgiu com base em estudos de leis e normas anteriores, que, por sua vez, não atendiam de forma clara regras sobre a privacidade de dados, bem como a Carta dos Direitos Fundamentais da Europa conhecida como "A Carta" e o Tratado de Lisboa, ambas já tratavam de dados pessoais, porém, com pouco detalhamento.

Uma preocupação importante para GPDR é o compartilhamento de informações entre os países, com uma finalidade bem específica e clara em casos de investigações, prevenções e/ou possíveis punições. O desafio então seria como fazer essa troca de dados sem ofender o direito à privacidade das pessoas, mesmo que fosse em prol de um bem maior, limitando-se, assim, à tramitação na esfera judiciária ou policial para efeitos de investigação de suspeitos. Porém, mesmo em casos de suspeitos, a lei é clara quando aos dados genéticos dos indivíduos, descrevendo como dados com alto risco de utilização para outros fins que não os citados na lei.

> Art. 39. [...] Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos sobre os quais tratam. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.. (REGULATION, 2018)

Outro ponto importante dessa lei é quanto ao consentimento por parte do titular sobre a utilização de seus dados, tratamento e guarda, deixando muito claro quem são os responsáveis pelos dados, bem como a finalidade da utilização. Há casos em que a anuência do titular poder ser ignorada, por exemplo, em razão de interesse público no que tange à saúde geral ou à segurança nacional. Uma vez que o titular dá ciência ou consente a salvaguarda dos seus dados, ele precisa saber como consultar esses dados ou a forma de disponibilização deles. Assim sendo, a GDPR trouxe como uma diretriz a "Transparência", na qual diz que o titular e o público a quem possa ter direito, deve ter a informação de forma clara e de fácil acesso (artigo 58).

Como nada é eterno, pode chegar o dia em que o titular não queira mais que seus dados fiquem em posse de terceiros, o que essa lei chama de "direito a serem esquecidos". Esse direito poderá ser exigido a qualquer tempo pelo titular dos dados. Porém, vale ressaltar que esse direito poderá ser desconsiderado nos casos previstos em lei, citados no artigo 65 dessa lei.

> Art. 65. [...] Exercício do direito de liberdade de expressão e informação; cumprimento de uma obrigação jurídica; exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento; interesse público no domínio da saúde pública; para fins de arquivo de interesse público; para fins de investigação científica ou histórica ou para fins estatísticos; ou para efeitos de declaração; exercício ou defesa de um direito num processo judicial. (REGULATION, 2018)

Mesmo nos casos citados acima, é direito do titular saber quem é o responsável pelo tratamento de seus dados, bem como a finalidade, o período e a destinação final. Respeitando sempre o direito da criança, a lei faz uma distinção entre os menores, ou seja, somente poderá ser dado o consentimento se a criança tiver idade igual ou superior a 16, sendo o consentimento ou não para crianças abaixo dessa idade de responsabilidade dos responsáveis legais. Porém, essa mesma lei deixa a cargo dos Estados Membros a disposição legal sobre o devido tratamento, desde que a idade da criança não seja inferior a 13 anos. De forma mais genérica, a GDPR prevê tratamento diferenciado para alguns dados, são eles: dados referentes à raça ou à etnia; opinião política; convicções religiosas ou filosóficas; filiação sindical; tratamentos genéticos; dados biométricos; sobre saúde; vida sexual ou orientação sexual.

> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (REGULATION, 2018)

Independente do tratamento ou da destinação, o GDPR prevê que o titular dos dados é o principal prejudicado em caso de má utilização, de utilização indevida ou de divulgação de seus dados. Dessa forma, a lei deixa claro sobre a comunicação ao titular, forma e prazo de até 72 horas para notificação. Para que não fique a cargo das empresas fazer a notificação ao Estado, a lei prevê que haja uma unidade de controle principal, a qual deve receber as notificações, analisar e gerar relatórios, entre outras atribuições.

Assim como a GDPR, a LGPD surgiu da necessidade de uma legislação mais detalhada e rígida sobre o tratamento de dados pessoais. Já havia, no ornamento jurídico brasileiro, legislação que tratava do assunto, porém não de forma detalhada e específica, como exemplo, o Marco Civil da Internet de 2014.

Partindo do princípio que a LGPD teve como lei base a GDPR, as diretrizes, princípios, nomenclaturas, responsáveis e sanções são muito próximas da Europeia. Para evitar redundância ao falar sobre diretrizes já tratadas na GDPR e que a LGPD aderiu da mesma forma, nesta seção do trabalho falaremos sobre as principais diferenças ou diretrizes que não estão na legislação europeia.

A legislação estabelece ainda que as organizações devem adotar políticas e metodologias para prevenir a ocorrência de danos de qualquer espécie aos dados tratados, devendo comprovar que atendem tais requisitos. Algumas tecnologias e metodologias são necessárias para viabilizar, garantir e prover a segurança necessária, de acordo com o contexto moderno de proteção de dados, para a aplicação e a aderência ao disposto na LGPD entre elas podemos citar:

- *Identity and Access Management* (IAM) - Solução de Gestão de Identidades e Acesso, ou seja, garantir que apenas as pessoas credenciadas e autorizadas irão acessar a informação de acordo com o grau de restrição, autorização essa que pode variar desde uma simples consulta até o backup e cópia de arquivos.
- *Master Data Management* (MDM): Gestão dos dados utilizados como referência ou base para uma visão única, contendo todos os dados necessários para a gestão de negócios, infraestrutura, tecnologia, financeira, entre outras.
- *Privacy by Design e Privacy by Default*: Consiste na incorporação de salvaguardas de privacidade e dados pessoais em todos os projetos desenvolvidos, exatamente antes, ou seja, agindo como forma de prevenção e não de tratamento da ação de alguma falha.

Essas soluções ou metodologias podem evitar ou minimizar os riscos, o que se torna muito necessário devido ao fato de a nova lei garantir ao consumidor/usuário uma série de direitos sobre suas informações e, além disso, uma série de deveres para as organizações no que tange à coleta, ao uso, à correção, à eliminação e, até mesmo, à portabilidade de dados.

Em relação ao tratamento dos dados pessoais, a LGPD repete o que já está mencionado na lei europeia, mas acrescenta algumas coisas importantes, como exemplo, relacionado ao consentimento do titular, menciona o "tratamento mediante vicio de consentimento", que se define como algo que o agente foi levado a fazer indiretamente contra sua vontade, seja por um erro de percepção da realidade ou até mesmo por ignorância sobre o assunto.

> Art. 171. Além dos casos expressamente declarados na lei, é anulável o negócio jurídico:
> I - por incapacidade relativa do agente; II - por vício resultante de erro, dolo, coação, estado de perigo, lesão ou fraude contra credores. (BRASIL, 2018)

Diferentemente da GDPR, que define explicitamente a idade para consentimento por parte de crianças, a LGPD diz apenas que poderá ser consentido por apenas 1 dos pais ou responsável legal. Em relação às penalidades administrativas, a LGPD descreve a punibilidade monetária em percentual e valor máximo, sendo até 2% do faturamento no último exercício, não podendo ultrapassar R$ 50.000.000,00 (Cinquenta milhões de reais), por infração. Porém, ainda que a devida lei regre de forma clara, deixa também algumas possíveis brechas para não aplicação das sanções, entre elas: " a boa-fé do infrator" e "a pronta adoção de medidas corretivas", dois casos em que se torna possível a exclusão de punibilidade.

No que se refere à autoridade de fiscalização, normalização e sanções, no Brasil foi criada a Autoridade Nacional de Proteção de Dados (ANPD), vinculada diretamente à Presidência da República. A composição dela difere um pouco dos demais cargos da Administração Pública federal, não havendo prazo mínimo ou máximo para o mandato dos membros do conselho. Vale ressaltar que essa regra não se aplica aos demais representantes do conselho, somente para os membros, ou seja, os demais terão mandato de 2 (dois) anos.

Dada a visão geral, para aprofundamento sobre o tema do trabalho, restringir-nos-emos a tratar do tópico "privacidade de dados", tratado em diversos pontos da LGPD. A privacidade de dados tem sido alvo de estudiosos, tanto no que tange ao que é a privacidade em si, quanto ao que é ou não privado. A privacidade é um direito já protegido na própria Constituição Federal, no artigo 5°, inciso X, que, em resumo, determina que os dados são pessoais e invioláveis, ou seja, é facultado ao titular das informações dar ou não autorização para qualquer uso por parte de terceiros, inclusive sob risco de pena para quem fizer o uso de tais informações sem prévia autorização.

> Art. 5º - CF - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 1988)

Seguindo o princípio da Constituição, a privacidade é algo inviolável, e como os dados fazem parte de sua privacidade, eles seguem a mesma lógica. Para tanto, há que se falar em quais são os dados, como devem ser tratados, armazenados e, se for o caso, até mesmo serem excluídos. Logo no início da LGPD, são definidos quais são os dados pessoais e os separa em dois tipos: "dado pessoal", que são dados que poderiam identificar ou deixar identificável o indivíduo; e "dado pessoal sensível", que pode gerar alguns transtornos em vários âmbitos, como racismo ou qualquer outra forma de segregação ou tratamento discriminatório.

> Art. 5º - LGPD - Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018)

Para efeito geral, trataremos dados pessoais e dados pessoais sensíveis apenas como "dados do titular". Sabendo que os dados pessoais são privados, a LGPD trouxe algumas diretrizes sobre o tratamento, o armazenamento e o descarte. O tratamento deverá ter uma finalidade específica, clara e não poderá ser feito sem o consentimento do titular dos dados, salvo em casos específicos da lei. Define-se como tratamento toda operação descrita do parágrafo 5°, inciso X da LGPD, bem como define-se o operador como responsável pelo tratamento dos dados pessoais em nome do controlador no inciso VII do mesmo artigo.

> Art. 5º - LGPD - Para os fins desta Lei, considera-se:
> [...]
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> [...]
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem 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. (BRASIL, 2018)

O armazenamento pode ser definido como todo e qualquer banco de dados, que pode ser físico ou lógico para a guarda de dados pessoais do titular, independentemente do local onde fica guardado e a forma, por completo ou dividido, assim definido no inciso IV do art. 5° da LGPD. A nomenclatura para o local pode ser variada de acordo com a área, podendo ser nomeada como: Banco de dados, Repositórios, Arquivos, etc. Para o trabalho em questão utilizaremos o termo repositório.

3. METODOLOGIA

Um primeiro passo na direção da proteção de dados é entender como as grandes empresas tem implementado as novas diretrizes da LGPD. Um jeito de conseguir isso é coletando dados das pessoas que trabalham nessas empresas para que se entenda melhor suas visões e as ordens que elas recebem para o tratamento de dados sensíveis.

Para isso, um instrumento de coleta deve ser utilizado e o principal meio utilizado são os questionários. Isso se dá pois esses são maneiras interessantes de agrupar variáveis diferentes de um mesmo indivíduo e, assim, utilizá-las em um mesmo estudo. Além disso, ao utilizar estruturas de correlação em agrupamento de perguntas de um mesmo assunto, a confiança desse instrumento aumenta (DANCEY; REIDY, 2013).

Com isso em mente, um questionário contendo 21 perguntas foi desenvolvido e enviado, por meio de e-mail e pelo aplicativo de mensagens WhatsApp e por meio de amostragem por conveniência, enviado a amigos de trabalho e acadêmicos, para várias instituições públicas e privadas, como AGU, Ministérios da Economia, Ministério da Justiça, STEFFANINI e Banco do Brasil. Ao final de um mês, foi feito o download da base de dados final com 43 respondentes.

Por fim, utilizando-se do software estatístico R, tabelas e/ou gráficos foram produzidos para cada pergunta na tentativa de se analisar as respostas em cada uma delas. Além disso, para os itens 3 e 4, foi feita uma análise extra, separando os respondentes de empresas públicas dos de empresas privadas.

4. PROPOSTA DO INSTRUMENTO DE PESQUISA

A pesquisa procurou identificar o conhecimento dos profissionais em 3 quesitos: Conhecimento da legislação (LGPD); Formas de armazenamento de dados; e Segurança da informação. O questionário contou com a colaboração de 43 respondentes, entre integrantes de instituições públicas e privadas, que responderam 21 questões conforme listadas na tabela 1. Os resultados foram avaliados, na maioria dos itens, segundo a escala de Likert, com as opções: 1) discordo totalmente;2) discordo; 3) indiferente (ou neutro); 4) concordo; e 5) concordo totalmente. Alguns itens abertos ou dicotômicos foram adicionados para que a coleta se tornasse mais abrangente.

Tabela 1. Lista de perguntas aplicadas no *Survey*

ID	Título das Questões
Q1	Você trabalha em instituição pública ou privada?
Q2	Você tem conhecimentos sobre as regras básicas da Lei Geral de Proteção de Dados (LGPD)?
Q3	Em relação ao tratamento de dados pessoais, sua empresa solicita autorização (consentimento) para os tratamentos dos seus dados?
Q4	O documento de consentimento informa sobre os dados que serão tratados (finalidade). Sua empresa solicita a assinatura desse documento?
Q5	Em relação a privacidade, sua empresa utiliza sistemas que permitem controlar acessos?
Q6	Você tem conhecimento sobre a forma que seus dados são armazenados?
Q7	Como é feita a guarda dos dados em sua empresa?
Q8	Existe algum aviso na intranet ou você recebeu algum aviso/alerta por e-mail informando sobre privacidade de dados?
Q9	Você tem conhecimento sobre dados anonimizados e para que servem?
Q10	Você tem conhecimento sobre ferramentas de segurança em sua empresa (Firewall, software de monitoramento, criptografias, antivírus, etc.)?
Q11	Sua empresa divulga técnicas de segurança ou possui alguma política de segurança?
Q12	Você já foi informado ou teve conhecimento de alguma tentativa de ataque cibernético que sua empresa sofreu (Transparência)?
Q13	Quais meios de segurança abaixo sua empresa utiliza: Políticas de Senhas, Controle de Permissão para instalação de ferramentas; VPN's; Firewall.
Q14	Você tem conhecimento se os seus dados pessoais são compartilhados com outros órgãos ou empresas?
Q15	Você já foi informado sobre o direito ao esquecimento sobre seus dados pessoais?
Q16	Você sabe a diferença entre "dados pessoais" e "dados pessoais sensíveis"?
Q17	Em suas atividades do dia a dia, você recebe orientações sobre a conformidade da LGPD de sua gerência?
Q18	Em relação a documentação, em suas atividades tudo é documentado? Ex.: Processos, arquitetura, gestão de segurança, controle de acesso, etc?
Q19	Sua empresa tem algum mecanismo de proteção ou contingência para casos de vazamento ou perda de dados?
Q20	Sua empresa possui algum procedimento de eliminação ou exclusão automática de dados?
Q21	Você tem algum comentário em relação às ações que sua empresa tomou para garantir a conformidade com a LGPD? Poderia descrever quais foram essas ações e quais são as suas percepções em relação a elas?

5. RESULTADOS E DISCUSSÕES

A Figura 1 apresenta o percentual de respostas que cada questão obteve, sendo que os 4 últimos itens (Q3_public, Q3_private, Q4_public e Q4_private) são relativas às combinações das questões 3 e 4 com os respondentes de instituições públicas e privadas. A pergunta Q1 Tabela 1, visa identificar o perfil de respondente pelo tipo de instituição ou corporação. Aqui, o intuito é fazer os cruzamentos das respostas e identificar nível de conhecimentos sobre a LGPD e as instituições as quais estão vinculados.

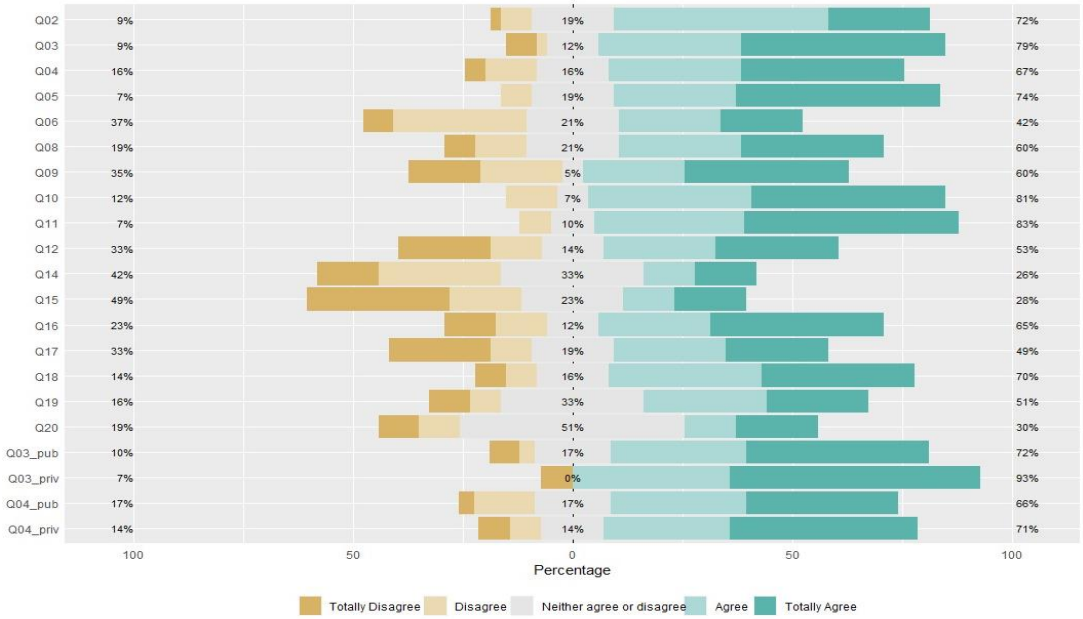

Figura 1. Apresentação do resultado por percentual de resposta

A partir dos resultados da Q3 da figura 1, em relação aos requisitos básicos, é fato que um dos principais itens do regramento, o "consentimento sobre o tratamento dos dados", não é de conhecimento dos profissionais. Observa-se que 17% dos entrevistados não foram informados por suas empresas sobre o tratamento ou não sabem desse regramento, como pode ser observado na Figura 1. Esse é um número bastante expressivo pela gravidade da diretriz, até mesmo pelo tempo em que a lei está em vigor. Ao fazer um relacionamento entre as perguntas Q1 e Q3 da Tabela 1, entre os respondentes do questionário que fazem parte de instituições públicas, 72% informaram que suas instituições informam sobre a necessidade de consentimento de tratamento dos dados pessoais. Já entre os respondentes de instituições privadas, esse número cresceu para 93%. Cruzando as questões Q1 e Q4, tivemos o resultado de 71% dos entrevistados de entidades privadas informando que sua empresa possui o termo de consentimento e no documento estava detalhado quais seriam os dados que seriam recolhidos e qual seria a finalidade. Já em empresas públicas, o índice de respostas foi 66%. A LGPD aplica um tratamento especial para os chamados "dados sensíveis". Nesse sentido, o dado preocupante que foi possível coletar na Q16 da Tabela 1 é quanto ao conhecimento sobre essa diferenciação dos dados. Como resultado, temos que 35% dos entrevistados informaram não saber a diferença entre os dados pessoais e dados pessoais sensíveis.

Quando passamos para área técnica em relação à segurança, privacidade e armazenamento, a pesquisa apresenta um dado importante. Na Q6 da Tabela 1, vemos que mais de 57% dos entrevistados responderam que não fazem ideia de como os dados são armazenados. Entre os que sabem a forma como os dados são armazenados, a Q7 da Tabela 1 mostra que 66% dos respondentes de entidades públicas disseram que a mais utilizada é o armazenamento na forma híbrida, enquanto 31% disseram utilizar o armazenamento local, e somente 3% em nuvem. Quando falamos de empresa privada, o percentual é alterado para 36% na forma hibrida, 29% de forma local 29% em nuvem, o que demonstra que as empresas privadas ainda são os maiores utilizados do armazenamento em nuvem, conforme apresentado na Figura 2.

Profissionais de Instituições Publicas				
ID	**Local**	**Nuvem**	**Hibrido**	**NSR**
Q7	31%	3%	66%	0%
Profissionais de Instituições Privadas				
ID	**Local**	**Nuvem**	**Hibrido**	**NSR**
Q7	29%	29%	36%	7%

ID-Identificador da Questão; NSR-Não Souberam Responder

Figura 2. Formas de armazenamentos mais utilizados por tipo de instituição

Ao perguntar sobre a anonimização de dados na Q9 da Tabela 1, os resultados mostram que não é de conhecimento de 35% dos entrevistados esse processo, sendo que 5% sequer conhecem ou sabem para que serve, permitindo, assim, inferir que os próprios profissionais de TI não estão preparados para a implantação completa da LGPD, conforme apresentado na figura 1. Com base nas respostas da Q13 na Tabela 1, é possível notar que as empresas fazem o básico, ou seja, controle de senhas, VPNs e Firewall. Porém, o questionário trouxe um dado importante para a segurança da informação, que é o controle de instalação de ferramentas por parte de usuários em suas estações de trabalho. Isso é uma falha antiga em políticas de segurança, visto que era comum ver usuários fazerem a instalação de ferramentas para facilitar o seu dia a dia. O problema desse fator é a forma de download e instalação, pois normalmente são softwares livres e retirados de sites não confiáveis, colocando em risco a segurança da estação de trabalho e, consequentemente, toda a rede da organização. Conforme mostrado na Figura 3, o questionário demonstrou que 69,8% não possuem a permissão para instalação de ferramentas, demonstrando que suas organizações já estão atentas à essa prática. Esse percentual é importante para o resultado de políticas de segurança e, apesar de não resolver todos os problemas, é uma forma de minimizar os riscos.

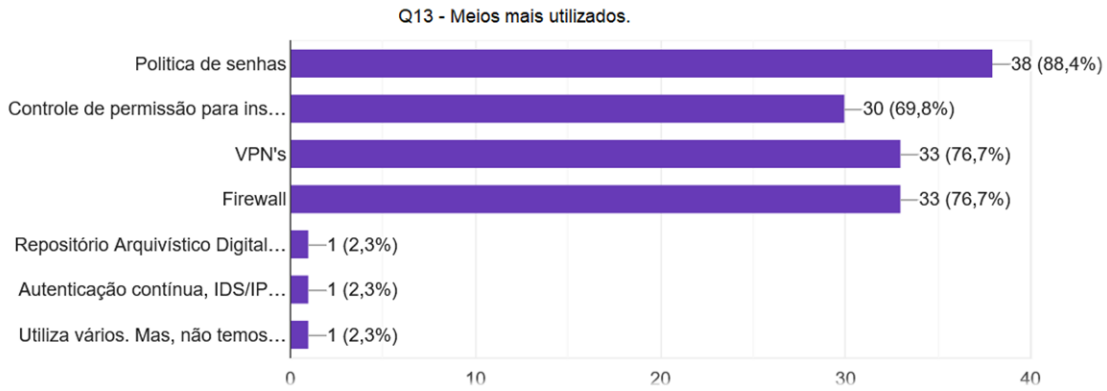

Figura 3. Meios de segurança mais utilizados

Diante dos resultados, a pesquisa mostrou indícios de que os profissionais não estão capacitados de forma correta e não estão prontos para adequação à legislação, desconhecendo tanto a legislação sobre direitos básicos como também as regras para garantir a privacidade e segurança dos dados dos usuários que estão previstas no regramento legal.

6. CONCLUSÃO

A LGPD é derivada da GDPR, que, por sua vez, foi criada baseada em leis anteriores que tratavam de segurança da informação e privacidade de dados, porém de forma mais genérica. Essa pesquisa mostrou que a LGPD detalhou, de forma mais ampla, a questão da privacidade de dados, deixando claro o que tem que ser feito para se garantir a segurança dos dados dos usuários, bem como os responsáveis e as possíveis punições em casos de vazamento ou tratamento indevido das informações que estão em posse de instituições públicas e privadas, concluindo-se que foi um avanço para a legislação brasileira.

Dando continuidade aos trabalhos, surgiu a necessidade de investigar o nível de conhecimento dos profissionais sobre a LGPD, segurança da informação e privacidade de dados. Foi realizado um *survey* que contou com 43 respondentes, sendo 14 de instituições privadas e 29 de instituições públicas. Dentre os principais resultados, alguns são mais relevantes e até mesmo preocupantes, como exemplo, 12 participantes não terem o conhecimento básico sobre a LGPD. No que tange a algumas obrigatoriedades básicas, ainda no sentido de tratamento de dados em que a lei prevê o prévio consentimento do titular sobre os seus dados, a pesquisa mostrou que 72% dos respondentes de entidades públicas e 86% de entes privados foram informados sobre o documento. No quesito armazenamento, a pesquisa detectou um problema que pode ser tanto de desconhecimento por parte dos profissionais quanto por falta de transparência de suas instituições, pois 57% dos entrevistados informaram desconhecer a forma de como seus dados são armazenados. Como os dados são considerados do titular, a pesquisa questionou sobre um direito importante que está contido na LGPD, o "direito ao esquecimento", e o resultado foi que 72% dos entrevistados desconhecem esse direito.

Com o estudo realizado sobre a legislação e apoiado pelo *survey*, é possível concluir que o repositório analisado não está em conformidade com a LGPD, uma vez que os resultados do questionário revelaram uma falta de conhecimento dos profissionais envolvidos nos projetos de tecnologia, bem como a falta de comprometimento por parte de gestores e instituições. Conclui-se ainda que se faz necessária uma ferramenta de apoio para ajudar no processo de adequação à LGPD.

AGRADECIMENTOS

Laboratório de Tecnologias para Tomada de Decisão -LATITUDE, da Universidade de Brasília, CNPq – Conselho Nacional de Pesquisa (312180/2019-5 PQ-2 e 465741/2014-2), do Ministério da Economia (005/2016 e 083/2016), do Conselho Administrativo de Defesa Econômica (CADE 08700.000047/2019-14), da Advocacia Geral da União (697.935/2019), do Departamento Nacional de Auditoria do SUS (23106.118410/2020-85), da Procuradoria Geral da Fazenda Nacional (23106.148934/2019-67).

REFERÊNCIAS

Albrecht, Jan Philipp. "How the GDPR will change the world." Eur. Data Prot. L. Rev. 2 (2016): 287.

Arquivos, C. C. N. de. Norma Brasileira de Descrição Arquivística - Nobrade. 2009.

Brasil. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988

Brasil. Lei nº13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Conarq, A. N. Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis.2015.

Cots, Márcio, and Ricardo Oliveira. "Lei geral de proteção de dados pessoais: comentada." (2020).Abiteboul, S. et al, 2000.

Da Silva, D. A., de Sousa Jr, R. T., de Oliveira Albuquerque, R., Orozco, A. L. S., & Villalba, L. J. G. (2021). IoT-based security service for the documentary chain of custody. Sustainable Cities and Society, 71, 102940.

Dancey, C.P.; Reidy, J. Estatística Sem Matemática Para Psicologia 5. ed. Porto Alegre: Penso, 2013.

De Vaus, David, and David de Vaus. Surveys in social research. Routledge, 2013.

Goddard, Michelle. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, v. 59, n. 6, p. 703-705, 2017.

Gomes, W. D. S.; Autran, M. D. M. M. Análise dos aspectos de confiabilidade do repositório digital arquivístico archivematica à luz da resolução nº 43 do conselho nacional de arquivos. Ciência da Informação em Revista, v. 7, p. 105–120, maio 2020.

Ramos, Pedro. A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD. Publicado em, v. 16, n. 07, p. 17, 2019.

Regulation, G. D. P. EU data protection rules. 2018

RLG-OCLC. Trusted Digital Repositories: Attributes and Responsibilities–An RLG-OCLC Report.[S.l.]: Research Libraries Group available at: www. rlg. org/longterm/repositories. pdf, 2002.

Rocha, Cláudia Lacombe. Repositórios para a preservação de documentos arquivísticos digitais. Acervo, v. 28, n. 2, p. 180-191, 2015.