O uso da criptografia a nível de campo para atender a desafios da LGPD

Juan Victor Dutra Juan, Felipe Pena Sales, Leonardo Zoccal Longato
Faculdade de Computação e Informática - Universidade Presbiteriana Mackenzie
São Paulo - SP - Brasil - 2021

Resumo: *Informações pessoais que produzimos diariamente a partir de interações em equipamentos tecnológicos são o combustível que sustenta o novo modelo dos negócios digitais. Tendo ciência disto, empresas e grandes grupos tentam cada vez mais obter o máximo de dados pessoais possíveis. A LGPD (Lei Geral de Proteção de Dados) surge com o intuito de regular as atividades de tratamento de dados pessoais no meio virtual brasileiro. Com a sua aprovação, todas as empresas que mantêm qualquer informação pessoal deverão se adequar às normas dispostas. A partir deste pressuposto, como as empresas poderiam se adequar tecnologicamente a fim de atender as necessidades regulamentadas pela LGPD? Analisando o contexto mencionado, um levantamento de possíveis tecnologias que consigam atender aos desafios da LGPD foi feito e a criptografia a nível de campo nos banco de dados conseguiu atender a todos os requisitos levantados. O objetivo deste trabalho é avaliar o uso da criptografia a nível de campo nos bancos de dados onde as informações são armazenadas como forma de proteger os dados e assim se adequar à lei de dados brasileira no que tange a segurança e integridade de dados pessoais. Um estudo de caso foi desenvolvido utilizando o recurso Always Encrypted para aplicar a criptografia a nível de campo em um banco de dados hospedado no sistema Azure. O Always Encrypted foi capaz de garantir a integridade e segurança dos dados em repouso.*

Abstract: *Personal information that we produce daily from interactions in technological equipment is the fuel that sustains the new model of digital businesses. Aware of this, companies and large groups increasingly try to obtain as much personal data as possible. The LGPD (General Data Protection Law) arises in order to regulate the activities of processing personal data in the Brazilian virtual environment. With your approval, all companies that keep any personal information must comply with the rules set forth. Based on this assumption, how could companies adapt technologically in order to meet the needs regulated by the LGPD? Analyzing the aforementioned context, a survey of possible technologies that can meet the challenges of LGPD was carried out and field-level encryption in the databases managed to meet all the requirements raised. The objective of this work is to evaluate the use of cryptography at the field level in the databases where the information is stored as a way to protect the data and thus adapt to the Brazilian data law regarding the security and integrity of personal data. A case study was developed using the Always Encrypted feature to apply field-level encryption to a database hosted on the Azure system. Always Encrypted was able to guarantee the integrity and security of data at rest.*

1. Introdução

Com a virada do milênio e as tecnologias se aproximando cada vez mais do nosso cotidiano, qualquer interação em algum dispositivo que utilizamos acaba gerando informações que são armazenadas em grandes bancos de dados das principais organizações e empresas. É inevitável dizer que estas informações podem ser consideradas a "grande mina de ouro contemporânea", e quem dispõe da capacidade de analisar e possuir a maior quantidade destas informações, detém o maior poder e influência na sociedade. "Na atual sociedade da informação, o bem mais valioso, o mais procurado, é justamente o que dá nome a essa nova sociedade: a própria informação" [Reinaldo Filho 2002]. Empresas, hoje em dia, negociam valores altíssimos por essas informações, e quem detém estes dados se torna o grande protagonista do mundo dos negócios digitais, como sustenta Danilo Duarte Queiroz:

> "Na 'nova economia', empresas ágeis são as que conseguem adquirir e administrar a maior quantidade possível de informação, no menor tempo e com a maior eficiência. Consequentemente, quem consegue prover e distribuir informação com maior competência, torna-se um 'fornecedor' concorrido e rico". [Queiroz 2002].

Tendo ciência da importância dessas informações para o mundo digital, muitas empresas e grupos tentam conquistar essas informações nos mais diversos meios, sendo eles legais; a partir de compras por empresas regulamentadas, ou ilegais; invadindo sistemas alheios, espionando empresas, grupos e países detentores dos dados ou se beneficiando de vazamentos alheios. A empresa japonesa Sony, teve a base de dados dos usuários de sua rede de videogames PSN (*Playstation Network*) divulgada por hackers na internet [Baker 2011], incluindo dados pessoais desses usuários (como histórico de compras, endereços de e-mails e número de cartão de crédito). O famoso episódio da agência de inteligência norte-americana NSA (*National Security Agency*) em 2013, que espionou e teve acesso a e-mails, mensagens pessoais e telefônicas de qualquer cidadão conectado à internet, onde até a ex-presidente da República Dilma Rousseff foi monitorada [G1 2013]. O episódio de vazamento dos dados da gigante da internet Yahoo!, com o vazamento de informações de mais de 500 milhões de contas [G1 2016]. Ou até o vazamento de dados de 223 milhões de brasileiros em janeiro de 2021, contendo informações que vão de CPF a imposto de renda de pessoa física [G1 2021].

Vale refletir quantos dados pessoais estão disponíveis nos nossos *smartphones* nesse exato momento; fotos da família, e-mails, mensagens pessoais, vídeos, acesso a vida bancária, dentre outros. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), 70,5% dos domicílios estavam conectados à rede em 2017:

> "Em 92,7% das residências, pelo menos um morador possuía telefone celular, enquanto o telefone fixo era encontrado em apenas 32,1% Com o crescimento do acesso à internet via telefone celular, de 60,3% dos domicílios em 2016 para 69% em 2017, cresce também a utilização desse instrumento para compras, pagamentos e homologações, além de navegação pelas redes sociais. Logo, o consumidor fica mais exposto ao fornecer número de CPF, telefone, endereço e outros dados pessoais, que podem ser utilizados de forma

> inadequada. A LGPD garante ao titular dos dados a possibilidade de verificar as condições de segurança oferecidas por quem os coletou por meio da exigência de um relatório." [Revista Segurança Eletrônica 2020].

Por essa razão, o foco das legislações mais modernas deste assunto é como o dado pessoal pode e deve ser tratado pelo privado e pelo público. É o que podemos encontrar na LGPD do Brasil.

Este trabalho tem como objetivo avaliar o uso da criptografia a nível de campo de bancos de dados como forma de proteger os dados e assim se adequar à LGPD no que tange a segurança e integridade de dados pessoais.

Na Seção 2, um aprofundamento da lei será feito, apresentando as suas principais cláusulas, objetivos, princípios e os temas de gestão de segurança da informação que rodeiam a sua concepção. Será feito também um levantamento dos impactos sociais e corporativos, trazendo os principais desafios que as empresas enfrentam para se adequar a lei. As Seções 3 e 4 abordarão a contextualização do trabalho, apresentando a sua metodologia, meios de pesquisas científicas, definição de objetivos do estudo de caso e levantamento de tecnologias. Na Seção 5, discutiremos como o uso e a implementação da criptografia a nível de campo de banco de dados nas empresas conseguiria suprir as necessidades de integridade e segurança de dados que a lei impõe. Por fim, a Seção 6 aborda a implementação do estudo de caso utilizando um banco de dados fictício com criptografia a nível de campo de banco de dados, juntamente com resultados e conclusões dos pontos levantados nas seções anteriores.

2. O que é LGPD?

A Lei Geral de Proteção de Dados Pessoais [Lei Nº 13.709 2018] sancionada em 14 de agosto de 2018 e que entrou em vigor a partir de dezembro de 2020, é uma legislação brasileira que tem como objetivo unificar todas as regras a respeito do uso de dados pessoais no Brasil ou de brasileiros, garantindo segurança jurídica das empresas e a privacidade dos dados pessoais de consumidores, trabalhando em prol da transparência e do consentimento. Na Figura 1, temos uma descrição de forma simples e objetiva dos conceitos desta lei. A LGPD tem como base a GDPR (Regulamento Geral sobre a Proteção de Dados) [EU 2016/679 2016], regulamentação europeia, e estabelece regras em respeito à coleta, compartilhamento e armazenamento de dados pessoais. A intenção é proporcionar a proteção dos dados, trazendo novas necessidades às empresas em relação ao uso e à segurança dos dados; que deverão suprir para que estejam alinhadas com a lei.

A LGPD traz consigo impactos em âmbitos social, cultural e corporativo, uma vez que ela traz à tona o tema da proteção e integridade de dados, causando indiretamente uma maior preocupação social a respeito do fornecimento e a finalidade de utilização das suas informações pessoais. Ela também influencia diretamente a maneira que as empresas deverão operar com os dados de seus clientes, expondo necessidades como a segurança ponta a ponta, transparência com o titular dos dados, possibilidade de fácil alteração ou exclusão dos dados, integridade dos dados armazenados e a possibilidade do titular dos dados conseguir consentir até onde aquela empresa poderá operar com as suas informações pessoais.

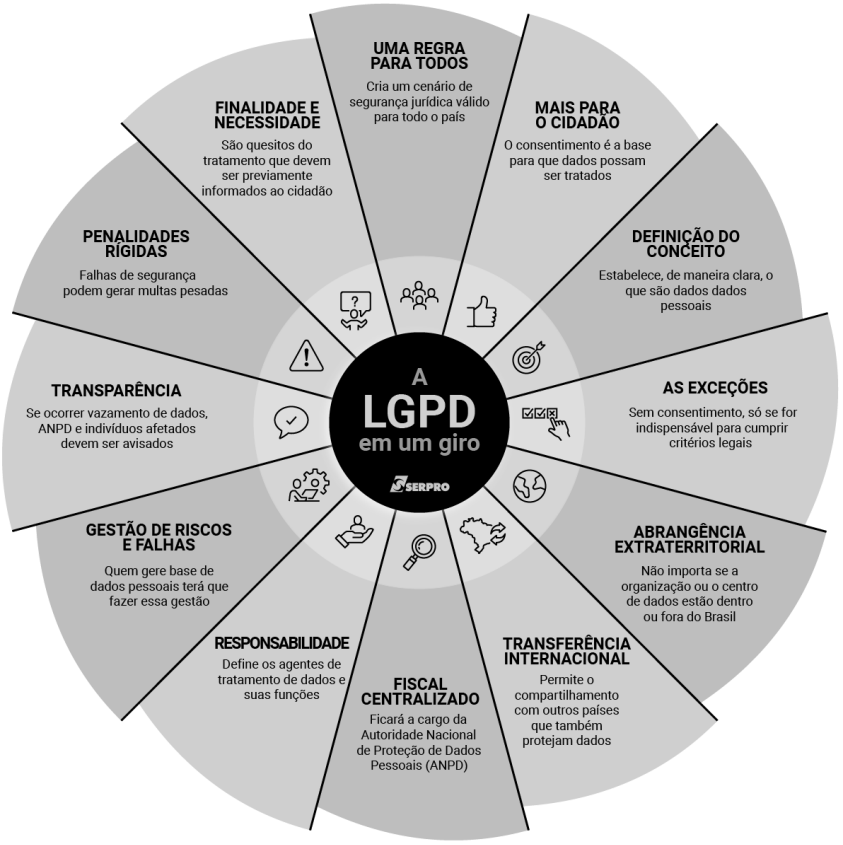

Figura 1 - A LGPD em um giro
(Fonte: SERPRO)

Como toda regulamentação, a LGPD possui os seus princípios, que podem ser descritos como: finalidade, adequação, necessidade, livre acesso, precisão**,** transparência, segurança e não discriminação. A **finalidade** diz que a coleta dos dados deve ser feita apenas para fins legítimos, informando sempre ao usuário o real motivo da mesma. A **adequação** e o **livre acesso** exigem que o detentor dos dados disponibilize todas as informações sobre a coleta e uso dos dados de forma honesta. Para evitar que o dado coletado esteja correndo riscos, os tópicos de **precisão**, **necessidade** e **segurança** são abordados na lei e obrigam que todas as medidas técnicas e administrativas sejam tomadas para garantir a segurança e evitar danos, furtos ou perdas; o detentor dos dados precisa manter e utilizar apenas dados essenciais, e precisa mantê-los preciso a todo momento.

2.1. Dificuldades de adaptação das Empresas à LGPD.

Com a lei em vigor, surge a preocupação de que as exigências para sua adequação causem prejuízo à competição em alguns setores e desincentivo à inovação, como aconteceu na Europa com a implantação da GDPR. O investimento alto e a burocracia para a adequação podem fazer com que pequenas e médias empresas tenham desvantagem em relação a grandes empresas. Além disso, o órgão responsável pela

aplicação de dezenas de artigos da lei ainda não foi constituído, e sem indicações de orçamento suficiente para custeá-lo [Ramos 2020].

A LGPD entrou em vigor em agosto de 2020, e já há casos onde a lei foi aplicada. Em São Paulo, uma juíza da 13ª vara de São Paulo condenou a empresa Cyrela, do ramo imobiliário, a pagar um valor de 10 mil reais a um cliente que teve os dados enviados a outras empresas [Angelo 2020].

Para garantir que a empresa está de acordo com a nova lei, sugere-se que as empresas tomem 7 passos, são estes; designar uma pessoa ou grupo internamente para garantir o cumprimento dos requisitos de proteção de dados, realizar um treinamento anual de privacidade e segurança para todos os funcionários, criar uma política de retenção de documentos, desenvolver um plano de respostas a incidentes em casos de violação dos dados, implementar uma política de dispositivos móveis para proteger e limitar o uso de dados confidenciais, investir em uma consultoria terceirizada para validar que sua empresa está de acordo com a LGPD e implementar um programa de garantia de segurança e privacidade de fornecedores [SC&H GROUP 2019]. Além dos 7 passos citados acima, é de responsabilidade institucional que cada empresa crie um Comitê de Segurança de Informação para analisar todos os procedimentos internos.

Toda empresa também deverá adotar o *Privacy by Design*, metodologia criada na década de 1990 pela comissária de Informação e Privacidade de Ontário do Canadá, Dra. Ann Cavoukian.

> "*Privacy by Design* é uma metodologia na qual a proteção de dados pessoais é pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais." [Cavoukian 2009]

A privacidade deverá estar presente na própria arquitetura dos sistemas, permitindo que o dono dos dados seja capaz de gerenciar a coleta e o tratamento dos seus dados pessoais de maneira segura e simples. A criptografia a nível de campo surge como uma solução que consegue atender às expectativas do *Privacy by Design*, uma vez que ela permite que o gerenciamento e compartilhamento dos dados sejam feitos de forma segura, pois os dados sensíveis estarão sempre criptografados.

2.2. Gestão da Segurança da Informação

A Segurança da Informação é um tema primordial a ser estudado caso queiramos compreender a LGPD. Com a utilização dos computadores em diversas organizações, passou-se a concentrar um volume muito grande de dados, consequentemente o grande volume dessas informações passou a ser um problema para a segurança, os riscos aumentaram com o uso dos microcomputadores a partir da utilização de redes locais e remotas e a disseminação da informática para diversos setores da sociedade.

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas

ou sua indisponibilidade." A ISO/IEC [17799:2005], em sua seção introdutória, define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Assim, podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua **integridade**, **disponibilidade** e **confidencialidade** a fim de garantir a continuidade do negócio e minimizar os riscos.

> • A **integridade** da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê la, seja de forma intencional ou acidental;
>
> • A **disponibilidade** garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário.
>
> • A **confidencialidade** da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do seu conteúdo;
>
> Sêmola (2003) ainda acrescenta a estes três objetivos o de:
>
> • **Legalidade** - garantia de que a informação foi produzida em conformidade com a lei;
>
> • **Autenticidade** - garantia de que em um processo de comunicação, os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

3. Metodologia de Pesquisa

Este trabalho tem uma natureza qualitativa a partir da pesquisa aplicada de tecnologias capazes de apoiar empresas com soluções para atender à LGPD. Para isso, foi realizado um estudo da lei de dados brasileira e assim escolher aspectos importantes a serem solucionados. Em seguida, foi realizado um levantamento bibliográfico para compreender a definição dos principais aspectos da área de Segurança da Informação: como integridade, disponibilidade e confidencialidade de dados.

Com todos os pontos da lei em mente, pesquisamos e levantamos tecnologias aderentes aos aspectos da lei mencionados, buscando referências no Google Acadêmico e utilizando como palavras-chave os desafios mencionados pela LGPD. Dentre as tecnologias levantadas, a criptografia a nível de campo de banco de dados foi escolhida. Um estudo de caso foi desenvolvido para simular a implementação da criptografia a nível de campo de banco de dados em um banco de dados fictício hospedado no sistema Azure a partir do programa *Always Encrypted*.

A pergunta a ser respondida neste trabalho é: *como uma empresa poderia adotar o uso da criptografia a nível de campo de banco de dados a partir do Always Encrypted para conseguir atender as expectativas de integridade e segurança dos dados perante a LGPD?* Nosso estudo de caso se baseia na implementação da criptografia a nível de

campo de banco de dados a partir do *Always Encrypted* em um banco de dados fictício que contém informações sensíveis de cartões de crédito. Iterações como consultas e atualizações de dados no banco criptografado foram feitas com o intuito de descobrir se os dados estarão seguros tanto em repouso como em trânsito.

4. Tecnologias com potencial de atender à LGPD

Para a realização do levantamento das tecnologias, pesquisamos por artigos no Google Acadêmico[1] e utilizamos como palavras-chave os desafios que a LGPD busca solucionar, mencionados na tabela 1. Partimos dessas necessidades para o levantamento e a escolha da tecnologia a ser implementada no estudo de caso:

- **Api REST**
  API REST, também chamada de API RESTful, é uma interface de programação de aplicações que segue conformidade com as restrições da arquitetura REST. Na maioria das vezes, as APIs são referidas como um contrato entre um provedor e um usuário de informações, estabelecendo o conteúdo exigido pelo consumidor (a chamada) e o conteúdo exigido pelo produtor (a resposta) [RedHat 2020]. Existem algumas tecnologias que conseguem garantir que os dados manipulados em APIs REST estejam seguros no momento do envio das requisições do lado do cliente, uma delas chama-se JWT (*JSON Web Token*) que consiste em um *token* de autenticação (*Bearer Token*) que valida que o cliente tem permissão de fazer requisições para a API, por exemplo, um sistema de login de usuário, o cliente envia uma requisição para o servidor passando usuário e senha, e o servidor retorna um status de sucesso e um *token*, esse token expira em um certo período de tempo que é definido pelo servidor, e com isso conseguimos garantir que apenas usuários autorizados consigam manipular os dados, e também ajuda a prevenir possíveis ataques de hackers, visto que para fazer requisições seria necessário, além do usuário e senha, o *token* de autenticação, garantindo a integridade, segurança e confidencialidade dos dados.

- ***Blockchain***
  Blockchain [Laurance 2019] é uma técnica de troca de dados criptografados em negociações de criptomoedas. Essa técnica consiste em gravar os dados de uma ou mais transações em um bloco de dados criptografado com *SHA-256*. *Blockchain* é um tipo de base de dados distribuída que guarda um registro de transações permanente e à prova de violação. A base de dados *blockchain* consiste em dois tipos de registros: transações individuais e blocos. Um bloco é a parte concreta da *blockchain* onde são registrados algumas ou todas as transações mais recentes e uma vez concluído é guardado na *blockchain* como base de dados permanente. Toda vez que um bloco é concluído um novo é gerado. Existe um número incontável de blocos na *blockchain* que são ligados uns aos outros - como uma cadeia - onde cada bloco contém uma referência para o bloco anterior. É esse sistema que permite o funcionamento e transação das chamadas criptomoedas, ou moedas digitais. A utilização da gravação de

[1] "Google Acadêmico." https://scholar.google.com.br/?hl=pt. Acessado em 19 mai.. 2021.

informações em transações de blocos criptografados com *SHA-256* consegue suprir as necessidades de integridade e segurança dos dados, uma vez que é praticamente impossível descriptografar este bloco de informação.

- ***SSH Safety File Transfer Protocol* ou Protocolo de Transferência de Arquivo por SSH (SFTP)**
  O SFTP é um protocolo de transferência de arquivos que utiliza o protocolo de segurança SSH-2 [Ellingwood 2018]. A sua principal diferença comparado com o FTP (*File Transfer Protocol*) é que utiliza criptografia em suas conexões através do estabelecimento de um enlace de SSH na porta 22, com funções hash de criptografia e descriptografia, autenticando tanto o servidor, quanto o usuário, que conseguem garantir uma maior segurança na importação e exportação de arquivos e protege os arquivos contra ataques sniffers (onde o atacante consegue ter acesso ao usuário e senha para acessar aquele sistema). O SFTP pode ser usado para armazenamento dos arquivos antes deles de fato serem inseridos no banco de dados com criptografia a nível de campo de banco de dados, garantindo a confidencialidade e integridade dos dados e possibilidade de alteração e exclusão dos dados.

- ***2FA* (*Two Factor Authentication* ou Autenticação de dois fatores)**
  A autenticação de 2 fatores é uma camada extra de segurança utilizada para proteger ainda mais o acesso a conta pelos usuários [Booking.com Partner Hub 2020]. Com ela, é possível ter certeza de que a pessoa que está tentando acessar a conta é realmente ela, e não outra pessoa tentando se passar por ela. Ao realizar a validação dos dados da conta para fazer o login, ao invés de acesso imediato será requerido mais algumas informações para validação, como um PIN (sigla de personal identification number, ou seja, número de identificação pessoal) enviado para um telefone autenticado, isso nos permite utilizar esta tecnologia perante a LGPD, uma vez que ela garante a segurança dos dados pois suas informações são criptografadas e a transparência, pois o usuário tem ciência da forma como o 2FA funciona, exigindo que ele confirme com uma senha de acesso que modifica-se a cada requisição do usuário.

- **Banco de Dados com Criptografia a Nível de Campo de banco de dados (*Field Level Encryption*)**
  A maioria dos serviços em nuvem que possuem banco de dados já possuem algum tipo de criptografia em sua arquitetura, seja no serviço como um todo ou apenas no banco de dados. A possibilidade de se criptografar não só o banco de dados como um todo a partir de chaves de acesso e permissões, mas também algumas colunas e valores sensíveis. A criptografia a nível de campo (*Field Level Encryption*) [Zope e Ahire 2015] de banco de dados condiz com a utilização de algoritmos de criptografia em colunas específicas de um banco de dados ao invés de criptografar o banco de dados por completo, permitindo que os usuários carreguem dados sensíveis com segurança de ponta a ponta em suas aplicações. Esta prática consegue atender a expectativa da transparência e utilização dos dados, assim como o fácil acesso do titular.

- **Assinatura Digital**
  Método de autenticação dos algoritmos de criptografia de chave pública que opera junto com uma função de hash. Sendo assim, quando tiver uma troca de informações criptografadas por meio de criptografia de chave pública, será gerado por meio de uma função de hash um resumo criptográfico, o que pode ser comparado a uma impressão digital, pois cada documento terá um resumo único [Macêdo 2012].
  Para confirmar uma assinatura digital é necessário realizar duas operações, decifrar a assinatura com a chave pública do signatário e calcular o resumo criptográfico. Se forem iguais, significa que foi gerada pela chave privada correspondente à chave pública utilizada na verificação e que o documento não sofreu alterações, e com isso a assinatura está correta. Se forem diferentes significa que pode ter havido modificações no documento ou na assinatura, com isso está errada. Com esta tecnologia, garantimos a segurança dos dados de ponta a ponta, uma vez que todo o tráfego de informações é criptografado, trazendo segurança e confidencialidade dos dados, além da possibilidade do dono dos dados acessar e visualizar seus dados.

Na Tabela 1 temos listadas as principais necessidades da LGPD e as tecnologias que as suprem. Mediante a implementação das tecnologias citadas acima, uma empresa conseguiria se adequar aos principais pontos cobrados pela LGPD a respeito da integridade e segurança dos dados dos seus clientes, uma vez que a união de um banco de dados com criptografia a nível de campo de banco de dados que possui restrição de acesso a dados sensíveis, com a utilização de ferramentas que controlam o acesso a esta informação como assinatura digital e *2FA*, a implementação de requisições de API REST para a coleta de dados e a utilização do SFTP para a transferência da mesma, conseguem fornecer um ambiente seguro e com vários enlaces de criptografia e autenticação de acesso, dificultando muito o processo de invasão e vazamento dos dados armazenados.

Tabela 1 - tabela comparativa de tecnologias e desafios que a LGPD busca solucionar.

Necessidades LGPD/Tecnologias	2FA	Blockchain	Field Level Encryption	Assinatura Digital	API REST	SFTP
Integridade de dados		X	X		X	X
Segurança ponta a ponta	X	X	X	X	X	X
Transparência com o titular dos dados	X		X			
Possibilidade de fácil alteração ou exclusão dos dados			X			X
Confidencialidade dos dados	X		X	X	X	X
Possibilidade do dono dos dados acessar e visualizar	X		X	X		

seus dados						
Política de retenção dos dados			X			

Após analisarmos as tecnologias e quais requisitos da LGPD elas suprem, escolhemos implementar em nosso estudo de caso a criptografia a nível de campo de banco de dados, pois ela pretende atender a todos os requisitos levantados da LGPD.

5. Criptografia a Nível de Campo de Banco de Dados

A criptografia a nível de campo de banco de dados (*Field Level Encryption*) [Zope e Ahire 2015] condiz com a utilização de algoritmos de criptografia (como RSA) em colunas específicas de um banco de dados ao invés de criptografar o banco de dados por completo, permitindo que os usuários carreguem dados sensíveis com segurança de ponta a ponta em suas aplicações. *MongoDB*[2] e *Amazon CloudFront*[3] foram os primeiros desenvolvedores desse método pioneiro de criptografia.

Atualmente, a criptografia a nível de campo de banco de dados também está presente no *Azure* e no *SQL Server* a partir do *Always Encrypted*[4]. Este método permite que campos individuais de um documento no lado do cliente sejam criptografados individualmente antes de enviá-lo ao servidor. Isso mantém os dados criptografados e seguros no lado dos provedores que hospedam o banco de dados, bem como de qualquer usuário que tenha acesso direto ao banco de dados. Como nem todos os dados armazenados são sempre confidenciais e importantes, a criptografia a nível de campo de banco de dados foi criada para permitir aos usuários a flexibilidade na escolha de quais tipos de atributos devem ou não ser criptografados. Essa criptografia garante que apenas os indivíduos que possuírem as credenciais necessárias consigam descriptografar os dados.

Segundo Anastasios Arampatzis, podemos aplicar o conceito da criptografia a nível de campo de banco de dados a um sistema de saúde:

> “O sistema de gerenciamento de clientes armazena informações pessoais dos pacientes, informações de seguro e registros médicos. Nenhum dos dados do paciente é público e, certos dados, como número do seguro social, número da apólice de seguro e medições de sinais vitais, são particularmente confidenciais e estão sujeitos à conformidade da GDPR / LGDP. É importante para a empresa e para o paciente que os dados sejam mantidos em sigilo e em segurança. Os médicos que trabalham neste provedor devem ter acesso total aos registros médicos de todos os pacientes, enquanto outro pessoal de apoio, como as recepcionistas, deve

[2] "Client-Side Field Level Encryption — MongoDB Manual." https://docs.mongodb.com/manual/core/security-client-side-encryption/. Acessado em 19 mai.. 2021.
[3] "Using Field-Level Encryption to Help Protect Sensitive Data ...." https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html. Acessado em 19 mai.. 2021.
[4] "Always Encrypted - SQL Server | Microsoft Docs." 30 out.. 2019, https://docs.microsoft.com/pt-br/sql/relational-databases/security/encryption/always-encrypted-database-engine. Acessado em 19 mai.. 2021.

> ter acesso a um conjunto limitado de dados, como informações de contato e os últimos quatro dígitos do número da segurança social." [Arampatzis 2020]

A criptografia a nível de campo de banco de dados no lado do cliente permite que os engenheiros de segurança especifiquem os campos de um documento que devem ser mantidos criptografados. Os dados confidenciais são criptografados / descriptografados de forma transparente pelo cliente e apenas comunicados para o servidor de forma criptografada. Este mecanismo mantém os campos de dados especificados seguros de forma criptografada no servidor e na rede. Embora todos os clientes tenham acesso aos campos de dados não confidenciais, apenas os clientes configurados apropriadamente são capazes de ler e gravar os campos de dados confidenciais. Isso é possível pois a criptografia a nível de campo de banco de dados utiliza dois tipos de chave no seu algoritmo de criptografia: a chave mestra e as chaves de colunas. As chaves de colunas são geradas a partir da mestra e para conseguirmos descriptografar os dados, precisamos da chave mestra, que por sua vez nos dá acesso às chaves das colunas.

Podemos relacionar o conceito do algoritmo de criptografia a nível de campo de banco de dados com uma casa: para você chegar na sala e acessar o conteúdo de dentro da casa, você precisará de duas chaves: a chave do portão da rua (chave mestra), e a chave de cada porta da casa (chave de coluna).

5.1 Always Encrypted

Always Encrypted é uma aplicação utilizada para proteger os dados pessoais armazenados em bancos de dados *SQL*, tanto do *Azure*, como do *SQL Server*, fornecendo recursos de computação confidencial, permitindo que o banco de dados processe algumas consultas em dados criptografados, mantendo o banco manipulável e garantindo a segurança.

Na prática o *Always Encrypted* permite que, ao configurar a criptografia para uma coluna, você pode especificar as informações do algoritmo de criptografia e chaves de criptografia usadas para proteger os dados na coluna (chaves de criptografia de coluna e chaves mestras de coluna):

- Uma chave de criptografia de coluna é usada para criptografar dados em uma coluna criptografada.
- Uma chave mestra de coluna é uma chave de proteção de chaves que criptografa uma ou mais chaves de criptografia de coluna.

Uma das maiores vantagens do *Always Encrypted* é garantir a segurança dos dados em um nível muito mais profundo que outras soluções, pois apenas os usuários e aplicações que possuem a chave mestra da criptografia conseguem acessar os dados, atingindo assim as necessidades impostas na LGPD de integridade dos dados. Também permite ao usuário acessar suas informações, alterá-las e removê-las, garantindo a transparência dos dados.

Além disso, a comunicação é criptografada tanto em trânsito, quanto em repouso. A diferença entre elas é que a em trânsito nos permite manter a criptografia das informações (dados, logs e as informações trafegadas pela rede) à medida que elas são movidas de um local para outro, ou seja, mesmo que os pacotes forem interceptados

durante a transmissão das informações, a informação ainda estará criptografada, diferente no caso dos dados criptografados em repouso. Sendo assim, o *Always Encrypted* garante a segurança ponta a ponta e confidencialidade dos dados, que são necessidades da LGPD. Porém o principal ponto pela escolha do *Always Encrypted* é o fato de sua utilização simplória, interface amigável e alta quantidade de documentação *on-line*, facilitando a sua implementação para este trabalho.

Um ponto extremamente importante quando aplicamos uma criptografia é entendermos quais dados foram criptografados, quanto tempo demorou e qual algoritmo de criptografia foi utilizado, para termos segurança de que o processo está sendo executado da maneira correta. Por conta disso, o *Always Encrypted,* quando implementado em um banco de dados, nos fornece um *log* com a descrição de todo o passo a passo que ele seguiu, as chaves de criptografia que foram criadas ou utilizadas e todas as colunas que foram criptografadas (Figura 2), facilitando assim o entendimento do que foi feito e, em caso de erros, qual foi o motivo.

```
mar 8 2021 19:04:48: Log opened. TraceLevel:Informational
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:Configurações do banco de dados de origem.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message: Nome do servidor de origem: tcc-lgpd.database.windows.net.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message: Nome do banco de dados de origem: bd-tcc-lgpd.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:Criar nova chave mestra.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message: Nome da nova chave mestra: CMK_Auto1.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message: Nova chave mestra no Azure Key Vault\\keys-bd-tcc-lgpd.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:Criar nova chave de criptografia.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message: Nova chave de criptografia: CEK_Auto1.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:Criptografar coluna CLIENTNUM.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Nome da tabela: clients.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Nome da chave de criptografia: CEK_Auto1.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Tipo de criptografia: Deterministic.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:Criptografar coluna Attrition_Flag.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Nome da tabela: clients.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Nome da chave de criptografia: CEK_Auto1.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Tipo de criptografia: Randomized.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:Criptografar coluna Customer_Age.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Nome da tabela: clients.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Nome da chave de criptografia: CEK_Auto1.
mar 8 2021 19:18:04 [Informational] WizardSummary: Message:   Tipo de criptografia: Randomized.
```

Figura 2 - log *de criptografia* do *Always Encrypted*

6. Estudo de caso da criptografia a nível de campo de banco de dados

Este projeto tem como objetivo demonstrar que o uso da criptografia a nível de campo de banco de dados é capaz de atender aos critérios citados na tabela (Tabela 1). Para realizar essa demonstração, agrupamos os critérios apresentados na Tabela 1 da seguintes formas: segurança (segurança ponta a ponta e confidencialidade dos dados); transparência (transparência com o titular dos dados, possibilidade de fácil alteração ou exclusão dos dados e possibilidade do dono dos dados acessar e visualizar seus dados) e integridade (integridade de dados e política de retenção dos dados) que as suprem como integridade e segurança dos dados, previstos na LGPD em uma perspectiva empresarial.

Entende-se o conceito de integridade como a garantia da exatidão da informação, assegurando que pessoas não autorizadas não possam modificá-la, adicioná-la ou removê-la. Segurança de dados refere-se a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A transparência para a LGPD se relaciona à garantia sobre a realização do tratamento e os respectivos agentes de tratamento de dados que operam as informações do indivíduo,

também diz respeito à autorização e acesso de suas informações a partir do legítimo interesse do titular dos dados.

Além de cumprir os requisitos da LGPD mencionados, é necessário que a aplicação possua um desempenho aceitável, que não inviabilize ou dificulte o uso do usuário à aplicação e o armazenamento das informações do cliente no banco de dados. Por conta disso, foi comparado o desempenho da aplicação nos escopos onde o fluxo de requisições e consequentemente de consultas no banco de dados é baixo ou alto, a fim de trazer uma perspectiva da performance de um banco de dados utilizando *Always Encrypted* quando sobrecarregado.

6.1. Projeto do Estudo de caso

Para conseguirmos representar a implantação da criptografia a nível de campo de banco de dados em um cenário empresarial, utilizamos um *dataset* fictício do site *Kaggle*[5] que simula uma base de serviços de cartões de crédito. Este conjunto de dados consiste em 10.000 registros de clientes contendo sua idade, salário, estado civil, limite do cartão de crédito, categoria do cartão de crédito e número do cartão de crédito.

Aplicamos a criptografia a nível de campo de banco de dados em colunas que consistem em informações pessoalmente identificáveis e sensíveis; como salário, limite do cartão de crédito e número do cartão de crédito. A partir disso, fizemos iterações de consulta, atualização e transferência de dados no banco hospedado na Azure, com o intuito de descobrir se a criptografia a nível de campo de banco de dados conseguirá atender as necessidades de integridade e segurança de dados exigidas pela LGPD. Também implementamos uma interface de *front-end* onde o usuário final poderá acessar a partir de um login e senha e visualizar os seus dados, a fim de garantirmos transparência com o titular dos dados.

Avaliamos a capacidade da tecnologia em prover os seguintes critérios: integridade dos dados, segurança ponta-a-ponta, transparência com o titular dos dados, possibilidade de fácil alteração e/ou exclusão dos dados, confidencialidade dos dados, possibilidade do titular do dados visualizar as informações armazenadas relacionadas a ele, facilidade de configuração, custo de arquitetura e tempo de desenvolvimento.

6.2. Implementação

A implementação do nosso estudo de caso, utilizando o *Always Encrypted* com criptografia em repouso, foi baseada na arquitetura cliente–servidor. O *back-end* tem a responsabilidade de receber e validar as requisições da interface do cliente, extrair a informação exata relacionada àquele cliente no banco de dados da *Azure* e descriptografar os dados em casa requisição. No *front-end,* implementamos uma interface que renderiza as informações descriptografadas após receber o pacote do *back-end* para o usuário final conseguir visualizar as suas informações a partir da validação do seu login e senha. Para que conseguíssemos implementar esta arquitetura, tivemos que utilizar alguns serviços disponibilizados pela *Microsoft Azure*, como:

---

[5] "Credit Card customers | Kaggle." 19 nov.. 2020, https://www.kaggle.com/sakshigoyal7/credit-card-customers. Acessado em 19 mai.. 2021.

- *Azure SQL Server*:
    - Servidor onde hospedamos um banco de dados *SQL* com os registros do *dataset* fictício do site *Kaggle*.
- *Azure Key Vault*:
    - Cofre de chaves, utilizado pelo *SQL* Server para armazenar com segurança a chave mestra da criptografia.
- *Azure Active Directory*:
    - Solução de gerenciamento do acesso de aplicativos e proteção de identidade avançada. Este serviço nos fornece um token de acesso ao *Key Vault*.
- *Azure Application Service*:
    - Hospedagem do *back-end*
- *Vercel*:
    - Hospedagem do *front-end*

O *back-end* foi implementado na linguagem de programação C# (ASP.NET), a sua escolha justifica-se em dois aspectos: conhecimento técnico da linguagem e documentação da utilização do *Always Encrypted* em C#. A implementação consiste em uma *API REST* seguindo a arquitetura de MVC (*Model View Controller*). Para o caso da criptografia a nível de campo, foi preciso adicionar uma classe (Figura 3) para lidar com o algoritmo de criptografia do *Always Encrypted*, essa classe tem a responsabilidade de acessar o *Azure Active Directory*, adquirir um *token* de acesso ao *Azure Key Vault* e instanciar um provedor de acesso ao mesmo.

```
public static class AlwaysEncryptedKeyVault
{
    private static ClientCredential _clientCredential;
    private static string applicationId ⇒ "e2f8a65e-e065-43e7-b536-d494bb5b2a09";
    private static string clientKey ⇒ "_1e81vl4zdGtr13Rg~~fUmH.hnNk8jDEwv";

    public static void InitializeAzureKeyVaultProvider()
    {
        _clientCredential = new ClientCredential(applicationId, clientKey);

        SqlColumnEncryptionAzureKeyVaultProvider azureKeyVaultProvider =
          new SqlColumnEncryptionAzureKeyVaultProvider(GetToken);

        Dictionary<string, SqlColumnEncryptionKeyStoreProvider> providers =
          new Dictionary<string, SqlColumnEncryptionKeyStoreProvider>();

        providers.Add(SqlColumnEncryptionAzureKeyVaultProvider.ProviderName, azureKeyVaultProvider);
        SqlConnection.RegisterColumnEncryptionKeyStoreProviders(providers);
    }

    private async static Task<string> GetToken(string authority, string resource, string scope)
    {
        var authContext = new AuthenticationContext(authority);
        AuthenticationResult result = await authContext.AcquireTokenAsync(resource, _clientCredential);

        if (result == null)
            throw new InvalidOperationException("Failed to obtain the access token");
        return result.AccessToken;
    }
}
```

Figura 3 - Classe que provê acesso ao *Azure Key Vault*.

A Figura 4 representa o fluxo de consulta e requisição de dados do cliente feito pelo *front-end*. Ilustramos como o algoritmo do *Always Encrypted* implementado no *back-end* criptografa o campo *client_id* para conseguir acessar o exato registro passado na aplicação web, uma vez que tanto o campo *client_id* como *credit_limit* estão

criptografados no banco de dados da *Azure*. Após encontrar o exato registro relacionado àquele *client_id* no banco de dados e retornar o valor do campo *credit_limit* criptografado, juntamente com a chave de criptografia de coluna (CEK) e o caminho para a chave mestra de coluna (CMK), o *back-end* faz uma consulta ao Repositório de chaves da *Azure* (*Azure Key Vault*) para conseguir encontrar a chave mestra de coluna (CMK) e conseguir descriptografar o valor do campo *credit_limit*. O Repositório de chaves da *Azure* então verifica o *token* de permissões da requisição do *back-end* e retorna o dado descriptografado como resposta para o *front-end*.

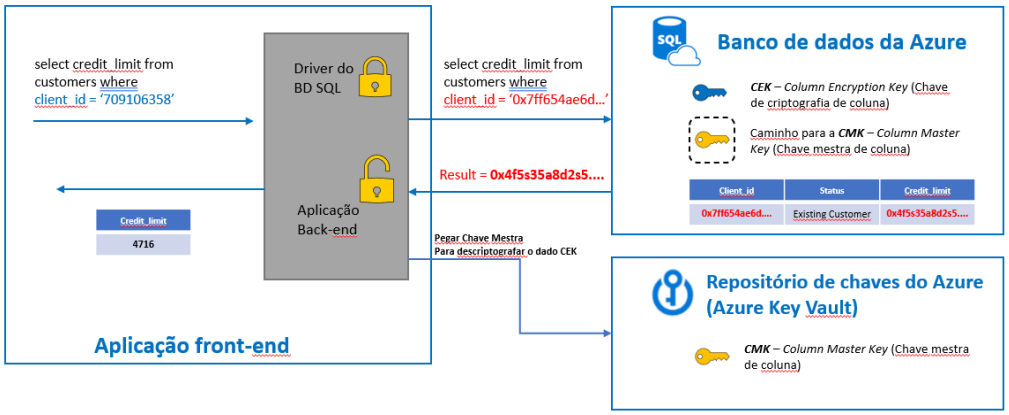

Figura 4 - Fluxo de consulta de dados da aplicação front-end a partir do *Always Encrypted*

O código completo utilizado para implementar o *back-end* deste estudo de caso está disponível em https://github.com/leolongato/backend-tcc-lgpd

Para a implementação *front-end*, utilizamos as linguagens de programação Next.Js e Typescript (Node.Js com tipagem), a escolha se justifica-se em três aspectos: conhecimento técnico das ferramentas, performance do framework Next.Js e facilidade e agilidade de desenvolvimento utilizando essas ferramentas. A implementação é uma página web, onde o cliente acessa com seu usuário e senha e é redirecionado para uma página que mostra suas informações pessoais que estão armazenadas no banco de dados.

A Figura 5 ilustra o fluxo de login da aplicação, onde o cliente envia para o servidor uma requisição *HTTP* Post, passando como corpo da requisição o usuário e senha. O servidor então retorna uma resposta validando o acesso, caso seja verdadeiro, ele é redirecionado para uma nova página, que busca os dados desse usuário e os mostra descriptografados.

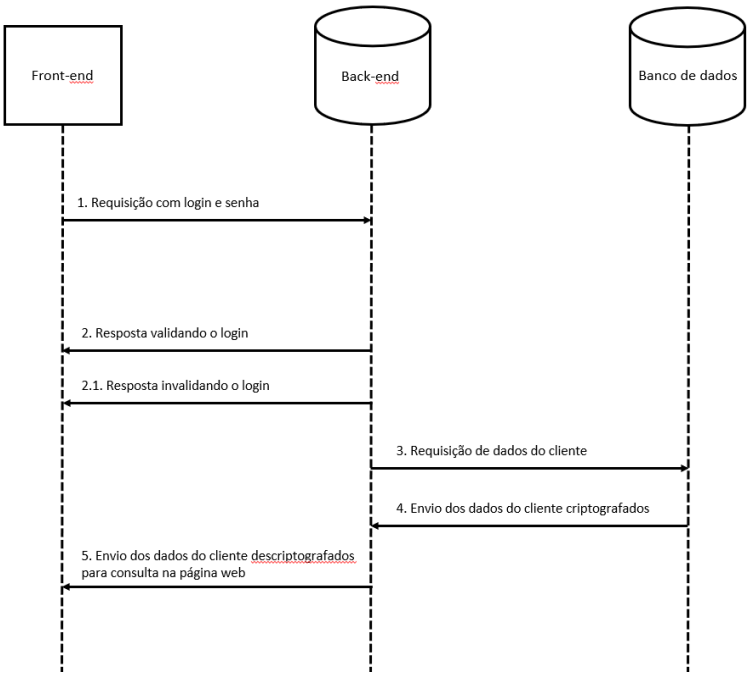

Figura 5 - Fluxo de login da aplicação.

O código completo utilizado para implementar o *front-end* deste estudo de caso está disponível em https://github.com/leolongato/frontend-tcc

6.3. Execução de consultas no Estudo de caso

Um ponto importante que o *Always Encrypted* nos garante é que o DBA (Administrador de Banco de Dados) não consegue visualizar as informações sensíveis através de consultas *SQL* no console, apenas as informações comuns (Figura 6). Portanto, apenas o detentor das informações sensíveis tem acesso a elas.

```
SELECT TOP 10 * FROM CLIENTS
```

133 %

Resultados | Mensagens

	client_id	credit_limit	status	age	gender
1	0x01000D9148C29168...	0x010F59C7886241C23...	Existing Customer	45	M
2	0x01001166B58A0EA1...	0x0124BD9A96143CB4...	Existing Customer	48	M
3	0x01001924FDB28503...	0x01E52753FD5818F4F...	Attrited Customer	38	F
4	0x01001E23D6103592...	0x01D0E1BBAEA5F80F...	Existing Customer	38	F
5	0x01003150B83759E0...	0x017ABE9E2950FD52...	Attrited Customer	61	M
6	0x0100344DEB182821...	0x01522A83EDF7EF7F...	Existing Customer	40	M
7	0x01003A91C9D72AA...	0x01CF924F9CB57E654...	Existing Customer	42	F
8	0x01003F03DF809B90...	0x015F0BA0C1D2F9A9...	Attrited Customer	37	M
9	0x01004672277DBC9B...	0x019A473DA66AD6B1...	Existing Customer	50	F
10	0x010048C4E86236EC...	0x01DB785820DAB21C...	Attrited Customer	32	F

Figura 6 - Consulta *SQL* feita no console do *Microsoft SQL Server Management Studio*.

A partir dos critérios levantados e descritos anteriormente para avaliação deste estudo de caso, conseguimos concluir:

- A integridade de dados consegue ser atendida neste estudo de caso utilizando a criptografia a nível de campo, pois uma vez que os dados são criptografados no banco de dados da *Azure* e não conseguimos visualizá-los de forma genuína sem possuírmos a chave mestra, consequentemente não poderemos alterá-los caso não possuímos as devidas chaves para sua descriptografia.
- A criptografia a nível de campo consegue garantir a segurança de dados em repouso pois impede que pessoas não autorizadas que não possuírem o acesso ao diretório específico da chave mestra acessem e visualizem os dados de maneira genuína.
- Conseguimos garantir a transparência para com o titular dos dados mediante a implementação da interface de visualização de dados, onde o usuário final conseguirá visualizar e alterar os dados de forma genuína.
- Para a utilização do *Always Encrypted* em cenários com alto fluxo de consultas por segundo, seria necessário avaliar se ele entrega performance, caso não entregue uma possível solução seria implementar um sistemas de filas de requisições no *back-end*, fazendo com que o banco de dados não fique sobrecarregado e consiga entregar respostas para todas as consultas.

6.4. Limitações

A principal limitação deste estudo de caso foi o custo dos serviços utilizados da *Microsoft Azure*, como: *Azure SQL Server, Key Vault, Active Directory* e *Application Service*. Para uma empresa conseguir implementar a tecnologia da criptografia a nível de campo em um sistema de banco de dados hospedado na *Azure*, ela terá que utilizar todos os serviços mencionados. Gostaríamos de ressaltar que não seria possível implementarmos uma solução utilizando os recursos da *Azure* se não fosse pela licença de estudante que a Universidade Presbiteriana Mackenzie disponibiliza para seus alunos. Agradecemos imensamente ao Mackenzie pela licença.

Pelo fato da utilização da criptografia em repouso no nosso estudo de caso, nosso *back-end* estará vulnerável a interceptações das respostas das requisições *HTTP*, visto que as informações estão descriptografadas e poderiam ser expostas, o que configura uma falha de segurança e de confidencialidade dos dados.

7. Conclusão

Com as exigências impostas pela LGPD, todas as empresas no Brasil deverão se adequar para garantir o *Privacy by Design*, ou seja, se adequando tecnologicamente e estruturalmente para conseguir atender as regulamentações de segurança da informação previstas na lei. Porém, alguns fatores como o alto custo destas mudanças tecnológicas e a falta de capacitação corporativa acabam dificultando empresas específicas de conseguirem chegar ao estado da arte no que tange às medidas impostas pela lei,

principalmente as micro e pequenas empresas. Este trabalho tem como finalidade apresentar a criptografia a nível de campo, a partir do *Always Encrypted* junto ao sistema e recursos da *Azure* como solução tecnológica a fim de auxiliar na conformidade e adequação perante as exigências de integridade e segurança de dados impostas pela lei.

A pergunta a ser respondida neste trabalho é: *Como uma empresa poderia adotar o uso da criptografia a nível de campo a partir do Always Encrypted para conseguir atender as expectativas de integridade e segurança dos dados perante a LGPD?* Para isso, realizamos um estudo de caso onde utilizamos um banco de dados fictício que contém informações sensíveis de cartões de crédito e o hospedados no sistema *Azure*, nele, implementamos a criptografia a nível de campo utilizando o algoritmo de criptografia determinística do *Always Encrypted*. Também desenvolvemos uma aplicação web onde conseguimos simular requisições para o banco de dados a fim de visualizarmos de forma genuína os dados relacionados àquele cliente.

Conseguimos concluir que uma empresa poderia adotar a criptografia a nível de campo para garantir a integridade e segurança de dados em repouso perante a LGPD, porém, para uma empresa assegurar que seus dados também estarão criptografados em trânsito, deverá ser implementado um novo enlace de criptografia do lado da aplicação web para impedir interceptações das respostas das requisições *HTTP*, visto que no estudo de caso apresentado, as informações estão descriptografadas e poderiam ser expostas quando chegam no *front-end*.

8. Referências

Angelo, T. (2020) "Juíza aplica LGPD e condena construtora que não protegeu dados de cliente",https://www.conjur.com.br/2020-set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao, Outubro.

Arampatzis, A. (2020) "What is Field-Level Encryption?", https://www.venafi.com/blog/what-field-level-encryption, Fevereiro.

Booking.com Partner Hub (2020) "O que é autenticação de 2 fatores (2FA)?", https://partner.booking.com/pt-br/ajuda/jur%C3%ADdico-e-segurança/seguranca/o-que-é-autenticação-de-2-fatores-2fa, Novembro.

Baker, L. B. e Finkle, J. (2011) "Sony PlayStation suffers massive data breach. 2011.",https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427, Setembro.

Covoukian, A. (2009) "Privacy by Design The 7 Foundational Principles", https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf, Setembro.

Cryptoid (2019) "O que é a Criptografia Assimétrica e como ela é essencial na segurança do Certificado Digital", https://cryptoid.com.br/certisign/o-que-e-a-criptografia-assimetrica-e-como-ela-e-essencial-na-seguranca-do-certificado-digital/, Setembro.

G1 (2013) “Documentos Revelam Esquema de Agência dos EUA Para Espionar Dilma”,http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html, Agosto.

G1 (2016) “Yahoo anuncia vazamento de dados que atinge 500 milhões de usuários”, http://g1.globo.com/tecnologia/noticia/2016/09/yahoo-anuncia-vazamento-de-dados-que-atinge-500-milhoes-de-usuarios.html, Agosto.

G1 (2021) “Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber”, https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml, Janeiro.

Ellingwood, J. (2018) “How To Use SFTP to Securely Transfer Files with a Remote Server” In: Digital Ocean Community, https://www.digitalocean.com/community/tutorials/how-to-use-sftp-to-securely-transfer-files-with-a-remote-server, Outubro.

Intersoft Consulting (2016) “GDPR: General Data Protection Regulation”, https://gdpr-info.eu/, Setembro.

Laurance, T. (2019) In: Blockchain for Dummies, 2nd Edition.

Macêdo, D. (2012) “Assinatura e Certificação Digital”, https://www.diegomacedo.com.br/assinatura-e-certificacao-digital/, Outubro.

Neroslavskaya, E. (2018) ”Azure SQL with PCF Spring Boot Applications”, https://medium.com/microsoftazure/azure-sql-with-pcf-spring-boot-applications-part-2-alwaysencrypted-bcea27010358, Janeiro

Netto, A. e Da Silveira, M. (2007) “Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas”, http://www.anpad.org.br/diversos/down_zips/33/ADI-B3180.pdf, Novembro.

Planalto Central (2018) “Lei Geral de Proteção de Dados Pessoais (LGPD). LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Artigo 5, inciso I, II”, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, Agosto.

Queiroz, D. D. (2002) Privacidade na Internet. In: REINALDO FILHO, D, Direito da Informática – temas polêmicos. 1ª Ed., Bauru, SP: Edipro,(p. 81 – 96).

Ramos, H. P. (2020) “O OTIMISMO COM A LGPD PODE SER ILUSÓRIO. ENTENDA POR QUE A NOVA LEI DE PROTEÇÃO DE DADOS JÁ COMEÇA CERCADA DE INCERTEZAS”, https://www.projetodraft.com/por-que-a-lgpd-ja-comeca-cercada-de-incertezas/, Agosto.

RedHat (2020) “O que é API REST?”, https://www.redhat.com/pt-br/topics/api/what-is-a-rest-api, Novembro.

Reinaldo Filho, D. (2002) Direito da Informática – temas polêmicos. 1ª Ed., Bauru, SP: Edipro(432 p.).

SC&H GROUP (2019) “7 Ways That Your Company Can Adapt to GDPR Regulations Right Now”, https://www.schgroup.com/resource/blog-post/7-ways-that-your-company-can-adapt-to-gdpr-regulations-right-now/, Novembro.

Senado Federal (2020) “Lei Geral de Proteção de Dados entra em vigor”, https://bit.ly/3qg6cFu, Setembro.

Microsoft (2020) “Configurar Always Encrypted usando Azure Key Vault”, https://docs.microsoft.com/pt-br/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell, Março.

Zope, S. e Ahire, S. (2015) Encryption Techniques for High Security. In: International Journal Of Scientific Engineering and Technology. Research, 4.