REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

LEI GERAL DE PROTEÇÃO DE DADOS APLICADA AO DIREITO ADMINISTRATIVO

GENERAL DATA PROTECTION LAW APPLIED TO ADMINISTRATIVE LAW

Osswald, Helendendof Rodrigues

Estudante, helendendof@gmail.com, Faculdade Futura;

RESUMO- O trabalho explora a relação entre a Lei Geral de Proteção de Dados e o Direito Administrativo, destacando desafios e implicações legais. Desde sua promulgação em 2018, a lei tem sido crucial para regular o tratamento de dados pessoais, afetando setores público e privado. A interseção entre Lei Geral de Proteção de Dados e Direito Administrativo é evidente, especialmente em princípios constitucionais como a legalidade, impessoalidade e publicidade. A lei reforça tais princípios ao estabelecer regras para o tratamento de dados no âmbito público. Temos também, a Lei de Acesso à Informação e o Processo Administrativo que são áreas de convergência entre Lei Geral de Proteção de Dados e Direito Administrativo, embora desafios de conformidade e segurança de dados persistam, especialmente na segurança pública. A aplicação da Lei Geral de Proteção de Dados na segurança pública apresenta desafios específicos, pois não pode impedir ou dificultar as atribuições constitucionais dos órgãos de segurança, mas deve garantir a proteção dos dados pessoais dos cidadãos. Diante desses desafios, é essencial que os órgãos públicos estejam em conformidade com a Lei Geral de Proteção de Dados, garantindo a transparência e a proteção das informações pessoais dos cidadãos. A responsabilidade do Estado é ampla, conforme estabelecido na Constituição Federal, e qualquer violação da Lei Geral de Proteção de Dados pode resultar em danos significativos aos direitos individuais e à dignidade da pessoa humana.

PALAVRAS-CHAVE: LGPD. Dados. Compartilhamento. Responsabilidade. Segurança Pública.

REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

ABSTRACT- The work explores the relationship between the General Data Protection Law and Administrative Law, highlighting challenges and legal implications. Since its promulgation in 2018, the law has been crucial in regulating the processing of personal data, affecting public and private sectors. The intersection between General Data Protection Law and Administrative Law is evident, especially in constitutional principles such as legality, impersonality and publicity. The law reinforces these principles by establishing rules for the processing of data in the public sphere. We also have the Access to Information Law and the Administrative Process, which are areas of convergence between the General Data Protection Law and Administrative Law, although compliance and data security challenges persist, especially in public security. The application of the General Data Protection Law in public security presents specific challenges, as it cannot prevent or hinder the constitutional duties of security bodies, but must guarantee the protection of citizens' personal data. Faced with these challenges, it is essential that public bodies comply with the General Data Protection Law, ensuring transparency and protection of citizens' personal information. The State's responsibility is broad, as established in the Federal Constitution, and any violation of the General Data Protection Law can result in significant damage to individual rights and human dignity.

KEYWORDS: LGPD. Data. Sharing. Responsibility. Public security.

1 INTRODUÇÃO

Na era contemporânea, caracterizada pela revolução digital e o advento da informação pós-industrial, a digitalização e a coleta massiva de dados surgiram como pilares cruciais para impulsionar o progresso tecnológico e econômico do país e do mundo. Proteger, preservar a privacidade e garantir a governança desses dados tornaram-se imperativos inegociáveis.

Nesta conjuntura, o governo busca incessantemente ferramentas eficazes para assegurar a segurança contínua desses dados, provenientes tanto de cidadãos quanto de servidores públicos. É nesse cenário que a Lei Geral de Proteção de Dados – LGPD – emerge, embasada em legislações e princípios constitucionais, estabelecendo diretrizes específicas para o tratamento de dados pessoais, visando salvaguardar a privacidade e os direitos individuais. Desde sua publicação em agosto de 2018 e com vigência a partir de agosto de 2020, a LGPD representa um marco no tratamento de dados pessoais, exercendo um impacto significativo nas atividades de coleta e tratamento de dados, seja por pessoas físicas ou jurídicas, no âmbito tanto público quanto privado.

A interseção entre a LGPD e o Direito Administrativo (DA) torna-se cada vez mais evidente no contexto do governo brasileiro. Enquanto a LGPD se destaca como uma legislação inovadora com repercussões jurídicas abrangentes, o DA, embora não seja codificado expressamente em um único documento oficial, desempenha um papel essencial em nosso sistema jurídico. Ambas as áreas regulam direta ou indiretamente as atividades dos agentes públicos, enfrentando desafios significativos na adaptação e implementação das normas da LGPD.

Nesse contexto, este artigo visa explorar a relação entre a LGPD e o DA, analisando os princípios da legalidade (Art. 37, caput, Constituição Federal de 1988), que exigem a conformidade estrita com as normas de proteção de dados. Também

ISSN 2763-9150

serão abordadas questões relacionadas à Lei de Acesso à Informação (Lei 12.527/2011), garantindo o direito dos cidadãos de acessarem informações públicas conforme a lei e suas alterações, além do Processo Administrativo (Lei 9.784/1999) e nas contratações públicas (Lei nº 14.133/2021), que demanda transparência, consentimento e proteção de dados em procedimentos de coletas de dados. Ademais, serão discutidas as implicações da LGPD nos desafios éticos e legais da coleta e uso de dados pessoais em atividades de segurança pública, bem como a responsabilidade civil do Estado (Art. 37, inciso 6º, da Constituição Federal de 1988), especialmente em casos de vazamento ou uso inadequado de informações pessoais.

.

2 MATERIAL E MÉTODOS

Esta pesquisa foi conduzida através de estudos e investigações online, utilizando métodos de pesquisa digital. Foram obtidas informações de sites e aplicativos que compilam, armazenam e compartilham dados de terceiros na internet, seja através de dados disponibilizados por órgãos públicos ou pelos próprios titulares dos dados.

Além disso, foram consultadas as bases de dados do site planalto.gov.br para obter informações atualizadas sobre leis e princípios constitucionais relevantes para este estudo.

Para complementar, foi conduzida uma pesquisa social utilizando um formulário digital, visando coletar informações de pessoas do meu círculo social. O objetivo era avaliar o nível de conhecimento das pessoas sobre o tema e verificar se já haviam sido vítimas de vazamento de dados pessoais na internet.

3 RESULTADOS E DISCUSSÃO

As atividades de tratamento de dados (segurança, transparência e compartilhamento) são cruciais tanto para o setor público quanto para o setor privado. Nesse contexto, a relação entre a LGPD e o princípio da legalidade, conforme delineado no artigo 37 da Constituição Federal de 1988, estabelece que a administração pública deve agir em estrita conformidade com a legislação vigente. Em outras palavras, as ações dos agentes públicos devem estar em conformidade com a lei em vigor.

No entanto, têm sido observadas falhas significativas por parte do Estado no cumprimento dessa obrigação. Um dos principais problemas está na falta de estrutura e capacitação adequadas para lidar com questões relacionadas à proteção de dados. Capacitar um agente público é fácil, mas difícil é verificar se o agente está utilizando as ferramentas adequadas e aplicando o que foi aprendido nos treinamentos. Muitas vezes, os órgãos públicos não dispõem de pessoal qualificado ou recursos suficientes para implementar medidas eficazes de segurança da informação. Isso resulta em vulnerabilidades que podem ser exploradas, colocando em risco a privacidade e a segurança dos dados dos cidadãos. Além disso, há uma falta de transparência e accountability no tratamento de dados por parte dos agentes públicos. Em muitos casos, informações pessoais são coletadas e utilizadas sem o consentimento adequado dos indivíduos (proprietários dos dados), violando seus direitos de privacidade. A falta de prestação de contas dificulta a identificação e responsabilização por eventuais violações de dados. Outra questão preocupante é a negligência na adoção de medidas de segurança cibernética. Com o aumento das

ISSN 2763-9150

ameaças digitais, é fundamental que os órgãos públicos implementem protocolos robustos para proteger os dados sob sua responsabilidade.

A LGPD reforça o princípio da legalidade ao estabelecer uma regra específica que se aplica ao direito público. Isso significa que qualquer ação relacionada a tratamento (movimentação em geral) de dados pessoais, pela administração pública deve ser realizada em conformidade com as exigências e princípios desta lei. Assim, a relação da LGPD e legalidade assegura que toda atividade de coleta, tratamento, armazenamento e compartilhamento de dados pessoais sejam realizados de forma transparente, responsável e dentro dos limites estabelecidos pela lei.

Seguindo com nosso artigo vamos analisar a Lei de Acesso à Informação (LAI) e sua relação com a LGPD, mas primeiro vamos abordar um breve conceito da Lei de Acesso à Informação. O objetivo da LAI é garantir a transparência das informações públicas e o direito de acesso à informação. Como previsto no art. 5º, XXXIII, art. 37, §3º, II e art. 216, §2º, da constituição federal.

> Art. 5º, XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (Regulamento) (Vide Lei nº 12.527, de 2011).
> Art. 37, §3º, II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII; (Incluído pela Emenda Constitucional nº 19, de 1998) (Vide Lei nº 12.527, de 2011).
> Art. 216, § 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem. (Vide Lei nº 12.527, de 2011).

É fundamental que os órgãos públicos assegurem o acesso a informações públicas de maneira incondicional. Este acesso não requer a apresentação de um motivo específico e pode ser solicitado por qualquer pessoa, seja ela física ou jurídica. Esta prática é essencial para garantir a transparência das informações governamentais e preservar o direito à informação. A única exceção se aplica às informações cujo sigilo seja absolutamente necessário, deve ter argumentação com base em lei. Ao adotar essa abordagem, os cidadãos têm a oportunidade de entender melhor o funcionamento do Estado e a utilização dos recursos públicos.

Conforme discutido anteriormente, a LGPD é uma lei recente que protege os dados pessoais e tem uma importância significativa na aplicação da LAI. Ambas as leis compartilham o princípio da transparência, mas a LGPD introduz uma nova exigência no compartilhamento de dados: a necessidade de consentimento explícito do titular dos dados para que o controlador e operador do banco de dados onde serão ou estão armazenados esses dados, possam realizar qualquer tipo de tratamento dos dados pessoais coletados. Além disso, é exigido que o compartilhamento de informações públicas seja feito com cuidado, aplicando a segurança dos dados pessoais. O controlador e operador é obrigado a verificar a conformidade com a LGPD antes de disponibilizar qualquer informação ao público externo ou publicar em páginas oficiais dos órgãos públicos (Diário Oficial, Página web Oficial do Governo). Portanto, mesmo no contexto da LAI, às informações públicas que contêm dados pessoais devem ser tratadas de acordo com as disposições legais da LGPD. Dessa forma, os

ISSN 2763-9150

documentos públicos que contêm dados pessoais devem ser protegidos, respeitando os direitos dos titulares dos dados. É fundamental que os órgãos públicos estejam em conformidade com ambas as leis, garantindo a transparência e a proteção das informações pessoais dos cidadãos e até mesmo de seus servidores.

Exemplo disso, o Portal da Transparência. É um recurso fundamental que revela a destinação dos recursos públicos de gastos com pessoal. Ao realizar uma consulta neste portal, é essencial que os dados pessoais permaneçam protegidos, sendo exibidas apenas as informações de interesse público e amplamente divulgadas. A Lei de Acesso à Informação (LAI) desempenha um papel crucial ao assegurar a transparência desses dados, mas temos também que aplicar os princípios da LGPD a este sistema. Deve também estabelecer mecanismos para o registro e o armazenamento histórico das pesquisas realizadas, possibilitando consultas posteriores para identificar os usuários que acessaram determinadas áreas do governo e coletaram dados.

O próximo tópico que abordaremos é bastante delicado: o Processo Administrativo (PA). Mas o que é um PA? É um procedimento formal e legal conduzido por órgãos públicos da administração direta e indireta para tomar decisões de interesse do Estado ou dos cidadãos que necessitam de um serviço público. Por exemplo: aplicar uma multa de trânsito, solicitar uma licença ou uma concessão de benefício, a abertura de uma licitação (um procedimento administrativo para selecionar a melhor proposta quando a administração pública deseja adquirir bens ou contratar serviços de terceiros), entre outros.

Com a evolução da tecnologia, a movimentação das informações digitais ganha grande foco nestas atividades. Os dados dos usuários são coletados para alimentar os procedimentos administrativos que são armazenados em sistemas informatizados dos órgãos públicos, que, por obrigação, devem oferecer segurança, proteção e transparência das informações, bem como disseminar a aplicação da LGPD e os direitos que os cidadãos têm na coleta de dados pessoais quando o agente público solicita em um atendimento obrigatório. No entanto, a realidade é diferente. Em fevereiro de 2024, a segurança e a proteção desses dados coletados ainda não são garantidas. Eles são compartilhados na internet e podem ser facilmente acessados por meio de buscadores. Não é necessário ser um hacker para obter um CPF, data de nascimento, nome completo, RG, entre outros dados sensíveis. Existem sites específicos que realizam a entrega deste serviço (consulta a CPF, RG, Contato celular, endereço, foto, nome da mãe…) e de forma legal (a coleta é de forma legal, mas violam a LGPD ao compartilhar os dados), pois os órgãos públicos deixam os dados expostos na internet e eles só realizam a coleta e junção dos dados em um único lugar e comercializam esses dados. Exemplos de site: Tudo sobre todos, Giga Dados, Consulta pelo CPF, BOT Telegram, Brasil Consultas, Sis Mix, CheckTudo, Deskdata.

Se você já participou de um concurso público ou realizou alguma atividade em órgãos públicos que caracteriza um ato administrativo, seus dados podem ter sido comprometidos. Com a criação da Lei Geral de Proteção de Dados (LGPD), espera-se que os dados coletados por órgãos públicos estejam protegidos. No entanto, essa proteção ainda não é 100% garantida, pois o governo está em busca de ferramentas para assegurar a proteção desses dados.

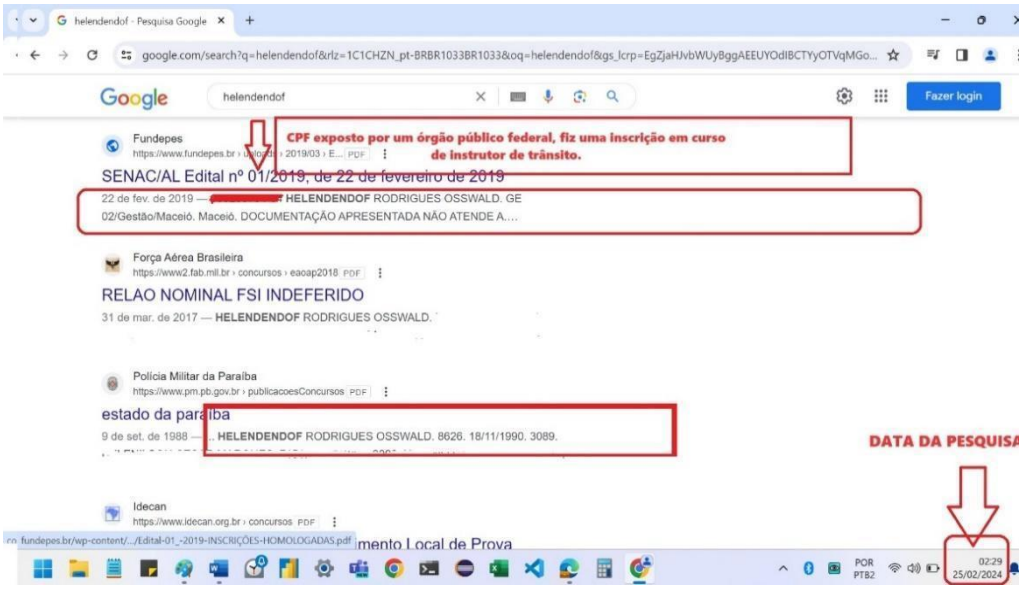
Para ilustrar essa falha, realizei uma pesquisa do meu nome no google chrome e obtive aproximadamente 443 resultados em 19 segundos. São muitos resultados, pois participei de vários concursos públicos, recebi multa de trânsito e realizei projetos

REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

com os governos estadual e federal. A imagem a seguir (figura.1) apresenta uma visão dessa falha nos sistemas governamentais do país.

Figura.1
Fonte: https://www.google.com/



O Processo Administrativo (PA) é uma ferramenta crucial para a coleta de dados dos usuários de serviços públicos. Simultaneamente, tornou-se um meio de compartilhamento de dados na internet, através das publicações nos diários oficiais do governo, tanto diretamente quanto indiretamente.

Forma Indireta: Existem indivíduos que mineram dados na internet para vendê-los a terceiros. Na era da informação e com a implementação da inteligência artificial, tornou-se muito mais fácil obter esses dados. Eles são comercializados para empresas que atuam em áreas como marketing, proteção de crédito e vendas diretas ao consumidor.

Forma Direta: O ato administrativo é publicado no diário oficial, por meio de sistemas interligados à internet que armazenam, leem e tratam os dados. No entanto, até a data desta pesquisa, o governo ainda não tem dado a devida atenção a este problema. Os dados pessoais de terceiros ficam expostos sem o consentimento dos proprietários desses dados sensíveis. Não é, porque, recebeu uma multa ou uma advertência do Estado que os dados pessoais devem ficar expostos para qualquer pessoa visualizar. A transparência deve existir, mas do que for cabível. Estamos a mais de quatro anos da publicação da Lei Geral de Proteção de Dados (LGPD), e ainda enfrentamos este problema nos sistemas governamentais.

Paralelamente ao PA, a Lei nº 14.133, de 1º de abril de 2021, que estabelece normas gerais para a realização de licitações e contratações no âmbito da administração pública direta e indireta, enfrenta o mesmo problema. A aplicação desta lei segue os princípios do artigo 37 da Constituição Federal, mas outros princípios da própria lei que estão previstos no artigo 5º.

> Lei nº 14.133, Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do

REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

Quando um serviço público é contratado, diversos procedimentos são realizados antes, durante e após a contratação. Todo esse processo ocorre por meio de atos administrativos. Como discutido anteriormente, existem problemas associados ao ato administrativo, e a licitação e gestão de contratos não são exceções. Enfrentamos os mesmos desafios com os sistemas governamentais que gerenciam e processam os dados pessoais dos usuários. Estes dados estão, explicitamente, expostos no diário oficial, no âmbito federal, estadual e municipal.

Figura.2
Fonte: https://diario.imprensaoficial.al.gov.br/ver-edicao?edition=26592&page=26&searchTerm=HELENDENDOF

LGPD aplicada à Segurança Pública

De acordo com o Art. 144 da Constituição Federal, a segurança pública é um dever do Estado, mas também um direito e responsabilidade de todos os cidadãos. Este artigo, estabelece que a segurança pública é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. Diversos órgãos atuam nesse sentido, incluindo a Polícia Federal, a Polícia Rodoviária Federal, a Polícia Ferroviária Federal, as Polícias Civis, as Polícias Militares e os Corpos de Bombeiros Militares, além das Polícias Penais Federal, Estaduais e Distrital. Além disso, a Lei Nº 13.675, de 11 de junho de 2018, desempenha um papel crucial na organização e funcionamento dos órgãos responsáveis pela segurança pública. Esta lei, que foi estabelecida nos termos do § 7º do Artigo 144 da Constituição Federal, cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e institui o Sistema Único

ISSN 2763-9150

de Segurança Pública (Susp). Estas medidas visam aprimorar a eficácia e a coordenação dos esforços de segurança pública em todo o país.

No contexto da segurança pública, a LGPD é aplicada com algumas ressalvas. Ela não pode impedir ou dificultar as atribuições constitucionais dos órgãos de segurança pública, ou seja, não pode impedir possíveis investigações ou operações de órgãos de segurança pública. O foco aqui não é a funcionalidade dos órgãos da segurança pública, mas sim as ações dos agentes públicos que compõem cargos nestes órgãos e que detêm os dados sensíveis dos cidadãos por meio de sistemas desenvolvidos para controle e fiscalizações em geral.

Apresentarei um incidente concreto que ocorreu comigo em outubro de 2021. Enquanto sinalizava minha intenção de virar à direita para entrar no condomínio onde resido, uma motocicleta realizou uma ultrapassagem pela direita em uma via de sentido único, desrespeitando o disposto no artigo 191 do Código de Trânsito Brasileiro. A manobra do condutor da motocicleta foi abrupta, chegando a se posicionar ao lado da porta do passageiro dianteiro do meu veículo, quase perdendo o controle ao transitar pelo acostamento, o qual apresentava irregularidades e altura considerável.

No dia seguinte, enquanto estava no meu local de trabalho, fui abordado por um indivíduo que se identificou como acompanhante de um policial. O indivíduo, aparentando ter cerca de 50 anos ou mais, solicitou uma conversa comigo e, durante o diálogo, detalhou informações pessoais a meu respeito, incluindo a data em que obtive minha Carteira Nacional de Habilitação (CNH), histórico de multas, endereço residencial atual e anterior, CPF, RG, data de nascimento e nome dos meus pais, além do histórico do meu veículo.

Essa divulgação de informações sensíveis levantou questionamentos sobre como tais dados foram obtidos pelo indivíduo em questão. Vale ressaltar que ele não se identificou formalmente como policial, embora estivesse acompanhado de um. A obtenção dessas informações somente seria possível mediante a abertura de um Boletim de Ocorrência (B.O.) na Delegacia Civil (PCAL) para investigações futuras pelos agentes da Polícia Civil. No entanto, é importante destacar que os policiais civis não estão autorizados a compartilhar informações detalhadas das partes envolvidas em incidentes (ocorrências), a menos que seja através do relato oficial presente no B.O. Após verificar a existência de algum B.O. em meu nome, constatei que não havia registro algum, o que corrobora a inexistência de qualquer infração, seja ela penal ou de trânsito, na situação mencionada.

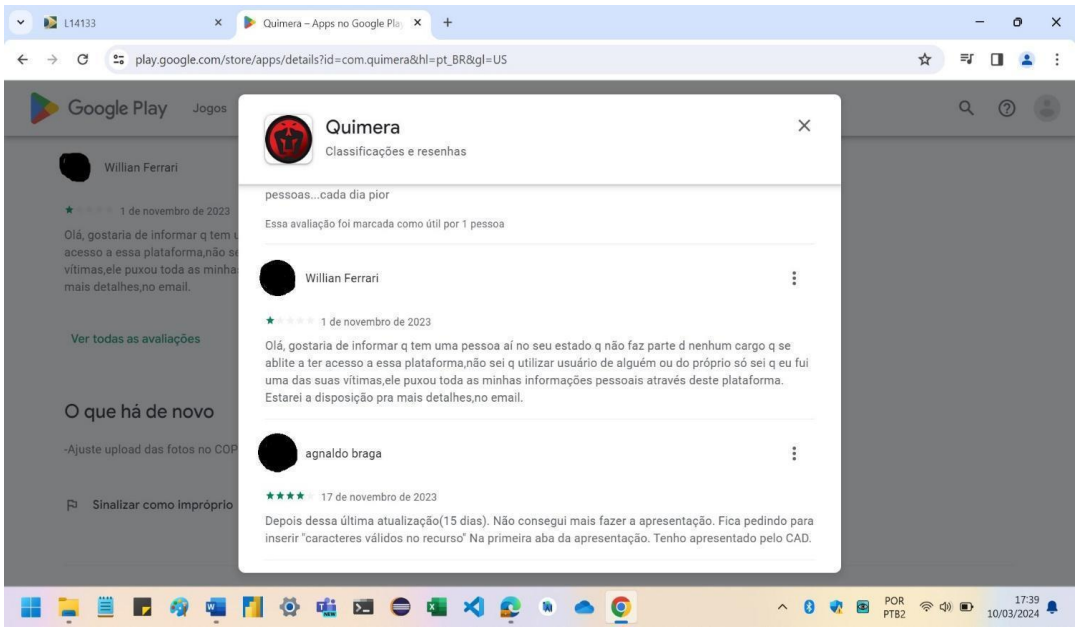
Uma possível fonte de obtenção dessas informações pode ser através de sistemas e aplicativos integrados da segurança pública, como o CAD (Cadastro de Ocorrências Policiais) e o Aplicativo Quimera, exclusivamente acessíveis a agentes da segurança pública do Estado de Alagoas. Enquanto o CAD é operado por atendentes, o Aplicativo Quimera possibilita que os próprios policiais realizem consultas em qualquer lugar e a qualquer momento, fornecendo dados pessoais de terceiros.

Por curiosidade, fiz algumas pesquisas sobre os sistemas apresentados. Verificando as mensagens de críticas do aplicativo Quimera vi algumas postagens interessantes, conforme imagens abaixo.

REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

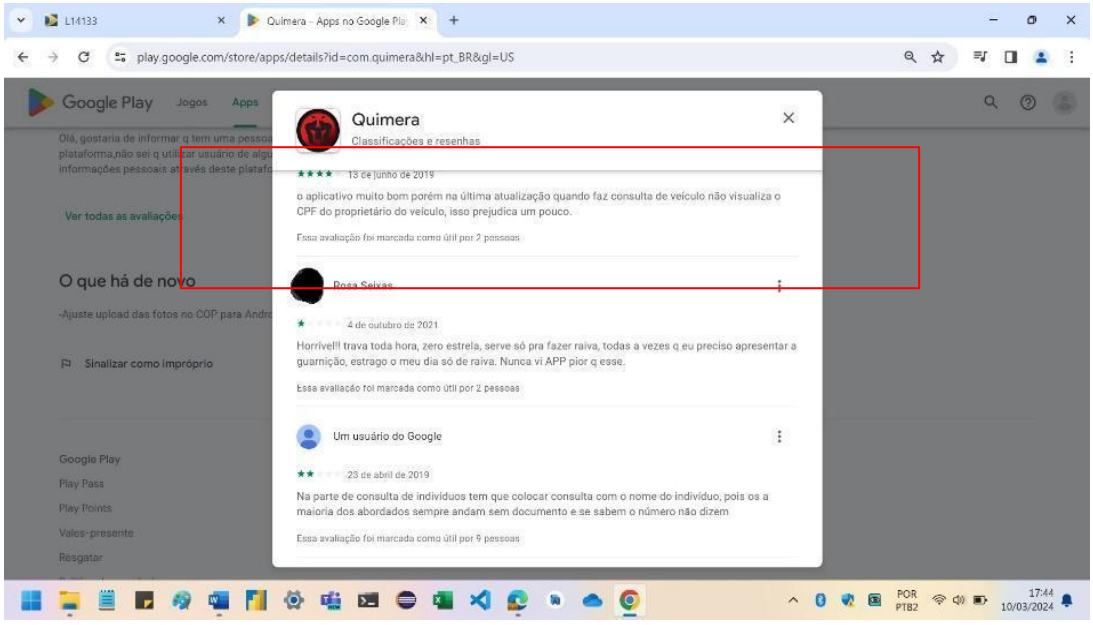
ISSN 2763-9150

Figura.3
Fonte: https://play.google.com/store/apps/details?id=com.quimera&hl=pt_BR&gl=US



Na imagem acima (figura.4), é criticado a não visualização do CPF na pesquisa no aplicativo.

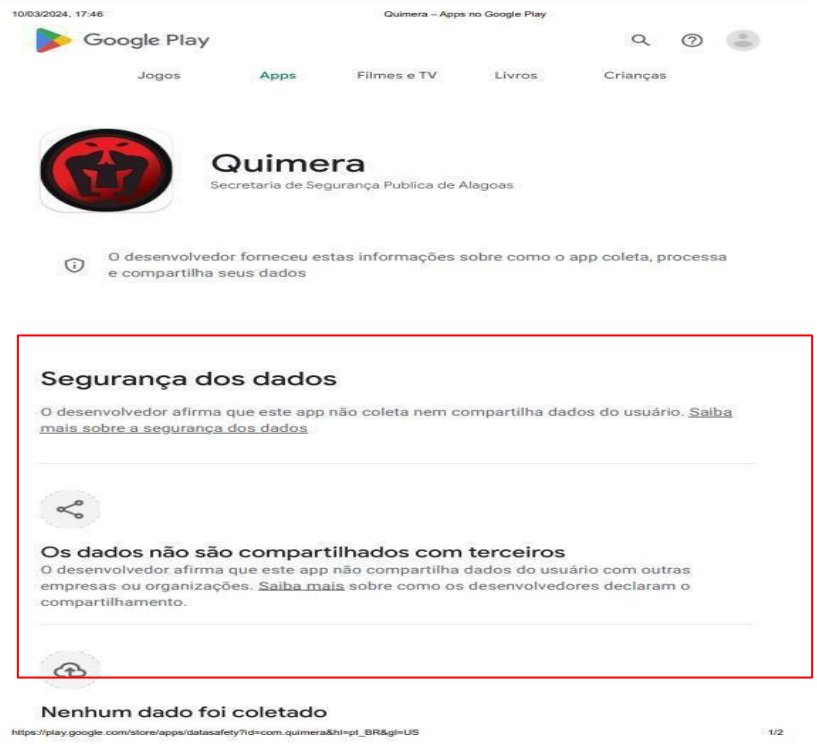
Figura.4
Fonte: https://play.google.com/store/apps/details?id=com.quimera&hl=pt_BR&gl=US



REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

Figura.5
Fonte: https://play.google.com/store/apps/details?id=com.quimera&hl=pt_BR&gl=US



Os desenvolvedores do aplicativo afirmam, figura.5, que não compartilham dados dos usuários e logo abaixo falam também que não compartilham dados com empresas ou organizações. De fato, eles podem não compartilhar os dados de quem utilizam o aplicativo, conforme sua política de privacidade (https://drive.google.com/file/d/1MOxnI7ZbQtkZXw46qeEEFsk1xWAO5nke/view?usp=sharing), mas os dados que são compartilhados por este aplicativo são os dados pessoais dos usuários do serviço público que são integrados na plataforma deste aplicativo. A finalidade do aplicativo é consultar as informações de terceiros para ter agilidade nas operações da segurança pública no estado de Alagoas. Porém, esta consulta deve estar em conformidade com a LGPD e garantir o consentimento e autorização dos proprietários dos dados, como expresso na LGPD. Vai retardar ou dificultar um órgão da segurança pública de agir? Não vai. Por outro lado, estando em conformidade com a LGPD vai garantir a segurança (proteção no compartilhamento) dos dados dos cidadãos usuários do serviço público.

Se realizarmos pesquisas na internet vamos encontrar diversas matérias falando sobre envolvimento de agentes públicos dos órgãos de segurança pública que cometeram crimes envolvendo dados pessoais de terceiros, comercialização ou outro tipo de crime usando dados coletados por sistemas informatizados do Estado. A seguir, figura.6 e 7, uma matéria publicada na internet de uma quadrilha formada por policiais, guardas municipais e pessoas civis que cometiam crimes de fraudes de cartão de crédito usando dados pessoais de terceiros. Prejuízo para comerciantes de mais de 1 milhão de reais no estado de Alagoas e Sergipe.

REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

Figura.6
Fonte: https://www.terra.com.br/noticias/brasil/policia/al-operacao-contra-cartoes-clonados-prende-19-pessoas,f640ac68281da310VgnCLD200000bbcceb0aRCRD.html

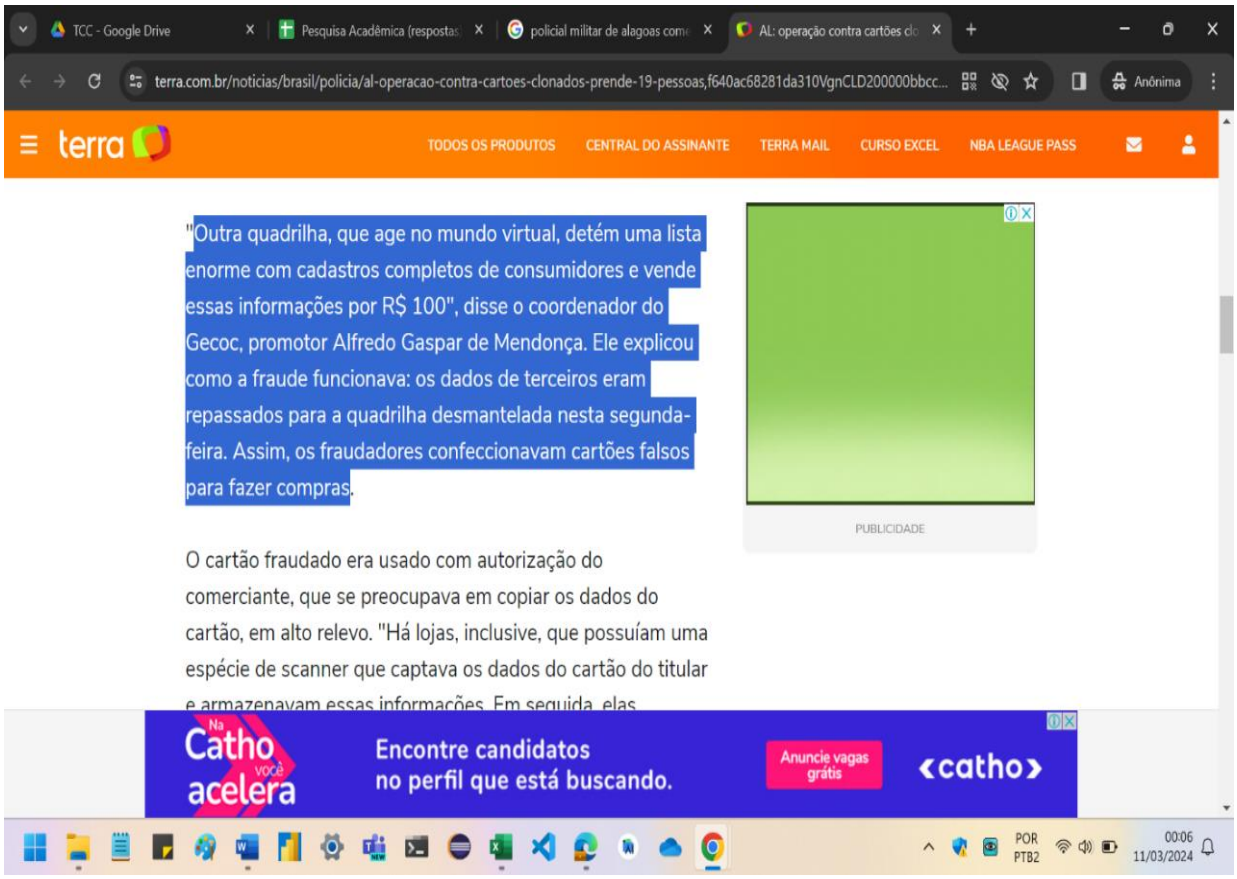
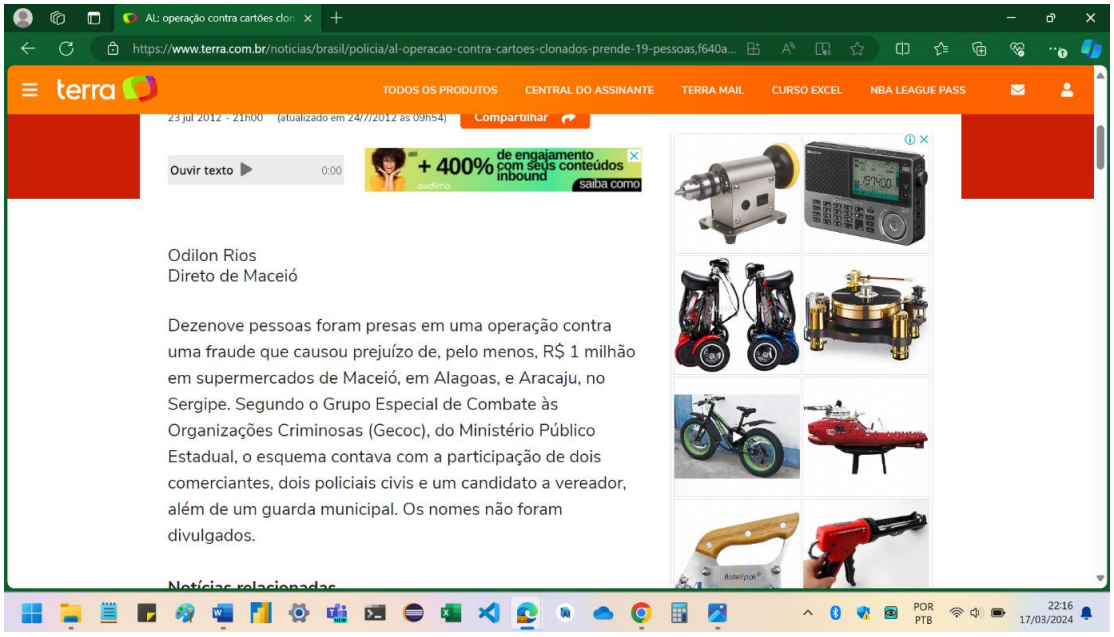


Figura.7
Fonte: https://www.terra.com.br/noticias/brasil/policia/al-operacao-contra-cartoes-clonados-prende-19-pessoas,f640ac68281da310VgnCLD200000bbcceb0aRCRD.html



REVISTA ELETRÔNICA CIÊNCIA & TECNOLOGIA FUTURA

ISSN 2763-9150

Conduzida uma pesquisa social utilizando um formulário digital, visando coletar informações de pessoas do meu círculo social. O objetivo era avaliar o nível de conhecimento das pessoas sobre o tema e verificar se já haviam sido vítimas de vazamento de dados pessoais na internet. Sem a obrigatoriedade de se identificar na pesquisa.

Figura.8
Fonte:
https://docs.google.com/spreadsheets/d/1S4KX3cmhuTGFYrdV9IpOPb1Nkm2GAYTFH1P13Pwcw8s/edit?usp=sharing

O aplicativo é um meio excelente nas atividades de segurança pública (aumenta a produtividade), mas os desenvolvedores e os órgãos responsáveis pela segurança pública têm a obrigação de assegurar a proteção, em conformidade com a LGPD, dos dados pessoais compartilhados na plataforma.

Uma maneira de alcançar isso é limitar o uso do aplicativo apenas durante o serviço ostensivo do agente público e monitorar as consultas em tempo real por uma equipe administrativa de analistas capacitados. Esta equipe teria a responsabilidade de registrar imediatamente os dados do usuário que realizou a consulta, além de acompanhar a finalidade, data e horário. Adicionalmente, seria incumbida de verificar a conformidade e legalidade do uso apropriado do aplicativo, bem como de outros sistemas com objetivos similares.

Sempre que possível, o cidadão abordado pelo agente público seria informado sobre a realização da consulta em seu banco de dados, recebendo a confirmação de que nada foi encontrado sobre ele.

Esse procedimento não apenas impediria que agentes públicos realizassem pesquisas ilegais, mas também estabeleceria um banco de dados para consultas futuras, contendo informações como o responsável pela consulta, data, hora, local e finalidade.

ISSN 2763-9150

Os dados consultados devem estar em conformidade com a LGPD. Temos o princípio da transparência aplicado. Por exemplo: ao realizar uma consulta de um cidadão, abordado por um agente da segurança pública, sem registro de infrações penais ou qualquer outro tipo de infração previstas no ordenamento jurídico brasileiro, não há a necessidade ter acesso a outros dados pessoais sensíveis do cidadão. Vamos lembrar que existem órgãos específicos que realizam investigações no âmbito da segurança pública, Polícia Civil e Polícia Federal.

Os sistemas informatizados buscam agilizar os serviços públicos, mas não devemos negligenciar a legalidade, transparência, as normas da LGPD e outros princípios legais.

Da responsabilidade do Estado

A responsabilidade do estado nas ações dos seus agentes públicos é ampla, pois qualquer ato lesivo ao vazamento de dados pessoais pode atingir diretamente a dignidade da pessoa humana. O Estado (órgão público) tem total responsabilidade por vazamentos ou compartilhamento indevido de dados pessoais guardados por eles. A constituição federal no artigo 37, §6 deixa bem claro esta responsabilidade dos danos causados por seus agentes públicos.

> **CF88, Art.37, §6º** As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

A LGPD prevê a responsabilidade do Estado no vazamento de dados pessoais. Embora a lei não contenha especificamente um artigo que trate exclusivamente dessa questão, ela estabelece princípios fundamentais, direitos dos titulares dos dados e obrigações para os controladores e processadores de dados, que se aplicam tanto ao setor público quanto ao privado.

O Artigo 42 da LGPD estabelece que o controlador e o operador serão responsabilizados por danos decorrentes do tratamento de dados pessoais, em casos de violação da legislação. Isso significa que, se houver vazamento de dados pessoais por parte de entidades governamentais, elas podem ser responsabilizadas pelos danos causados aos titulares dos dados.

Além disso, o Artigo 48 da LGPD estabelece que o controlador deverá comunicar ao titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados. Isso implica que, em caso de vazamento de dados pessoais, o Estado tem a obrigação legal de informar tanto os indivíduos afetados quanto a autoridade reguladora.

4 CONCLUSÃO

A intersecção entre a Lei Geral de Proteção de Dados (LGPD) e o Direito Administrativo apresenta um cenário complexo e desafiador para os órgãos públicos no Brasil. A implementação efetiva e a conformidade com essa legislação enfrentam uma série de obstáculos, desde a falta de estrutura e capacitação adequadas até a negligência na adoção de medidas de segurança cibernética. É crucial que a

ISSN 2763-9150

Autoridade Nacional de Proteção de Dados (ANPD) estabeleça diretrizes e orientações anuais para os agentes de tratamento de dados (Controladores e Operadores), a fim de garantir a compreensão e o cumprimento adequado das disposições da LGPD. Isso pode ser feito por meio de congressos e conferências que reúnam especialistas jurídicos em proteção de dados, sociólogos e psicólogos, para desenvolver ferramentas e estratégias de adequação da LGPD no país.

É fundamental que as ilegalidades identificadas sejam corrigidas, e para isso, a ANPD deve realizar fiscalizações regulares e aplicar sanções disciplinares para corrigir possíveis irregularidades, incentivando a conformidade com a lei. A LGPD representa um marco crucial na proteção dos dados pessoais dos cidadãos, estabelecendo obrigações claras quanto à transparência, consentimento e segurança no tratamento dessas informações.

É crucial que os órgãos públicos ajam prontamente para garantir a conformidade com a LGPD. Isso envolve a criação de leis e decretos regulatórios para governar o uso de ferramentas de gestão, controle e fiscalização, como aplicativos e sistemas informatizados que lidam com diversas informações. Além disso, é essencial promover a conscientização e a capacitação dos funcionários públicos, juntamente com investimentos em infraestrutura e tecnologia adequadas para salvaguardar os dados pessoais.

A responsabilidade do Estado na proteção dos dados de seus cidadãos é inegável, e qualquer falha nesse aspecto pode acarretar em danos significativos, conforme estabelecido na Constituição Federal e na LGPD. Portanto, é fundamental que medidas concretas sejam tomadas para garantir a integridade e a segurança das informações pessoais dos indivíduos, respeitando seus direitos fundamentais e promovendo uma gestão transparente e responsável dos dados públicos.

Para denunciar o descumprimento da LGPD, recomendo acessar o canal de denúncias e reclamações disponibilizado pela Autoridade Nacional de Proteção de Dados através deste link: Denúncia/Petição de Titular — Autoridade Nacional de Proteção de Dados (www.gov.br)

4 AGRADECIMENTOS

Agradeço ao meu filho, cujo amor, compreensão e apoio foram fontes inestimáveis de motivação durante todo o processo de elaboração deste trabalho. Sua existência me faz querer superar todas as dificuldades e obstáculos que porventura venham a cruzar meu caminho. Obrigado por ser uma parte tão importante da minha jornada acadêmica e pessoal. (PL)

REFERÊNCIAS

Brasil. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 14 de abril de 2024.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF, 2018. Disponível em:

ISSN 2763-9150

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 14 de abril de 2024.

Brasil. Lei nº 12.527, de 18 de novembro de 2011. Dispõe sobre o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 14 de abril de 2024.

Brasil. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília, DF: Presidência da República, 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/LEIS/L9784.htm>. Acesso em: 14 de abril de 2024.

Brasil. Lei nº 14.133, de 1º de abril de 2021. Estabelece normas gerais para a realização de licitações e contratações no âmbito da administração pública direta e indireta. Brasília, DF: Presidência da República, 2021. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm>. Acesso em: 14 de abril de 2024.

Brasil. Lei nº 13.675, de 11 de junho de 2018. Institui a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e cria o Sistema Único de Segurança Pública (Susp). Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm>. Acesso em: 14 de abril de 2024.

Google Play Store. Quimera. [Aplicativo de smartphone]. Disponível em: <https://play.google.com/store/apps/details?id=com.quimera&hl=pt_BR&gl=US>. Acesso em: 14 de abril de 2024.

Quimera. Política de Privacidade. Disponível em: <http://seguranca.al.gov.br/quimera-politica-de-privacidade/>. Acesso em: 14 de abril de 2024.

Secretaria de Segurança Pública de Alagoas. Formulários. Disponível em: <http://seguranca.al.gov.br/formularios/>. Acesso em: 14 de abril de 2024.

Secretaria de Segurança Pública de Alagoas. Termo de Responsabilidade de Inclusão de Senhas - Quimera. Disponível em: <http://seguranca.al.gov.br/wp-content/uploads/2019/02/TERMO-DE-RESPONSABILIDADE-DE-INCLUS%C3%83O-DE-SENHAS-QUIMERA.pdf>. Acesso em: 14 de abril de 2024.

Secretaria de Segurança Pública de Alagoas. Investimentos em novas tecnologias garantem agilidade nas operações policiais em AL. Disponível em: <http://seguranca.al.gov.br/noticia/2019/06/04/investimentos-em-novas-tecnologias-garantem-agilidade-nas-operacoes-policiais-em-al/>. Acesso em: 14 de abril de 2024.

ISSN 2763-9150

Secretaria de Segurança Pública de Alagoas. Termo de Responsabilidade de Inclusão de Senhas - CAD. Disponível em: <http://seguranca.al.gov.br/wp-content/uploads/2017/01/TERMO-DE-RESPONSABILIDADE-DE-INCLUS%C3%83O-DE-SENHAS-CAD.pdf>. Acesso em: 14 de abril de 2024.

Secretaria de Segurança Pública de Alagoas. Sistema CAD (Controle de Abordagem Digital). Disponível em: <https://gestor.cad.seguranca.al.gov.br/app/cad/cad_gestao_login/>. Acesso em: 14 de abril de 2024.