DAS CONSEQUÊNCIAS JURÍDICAS DOS ERROS COMETIDOS PELOS AGENTES DE TRATAMENTO DE DADOS: OS HOMÔNIMOS.

Rosemary Carneiro da Silva Rodrigues
Filha de Marinalva dos Santos Silva e Britivaldo Carneiro da Silva
E-mail: rosemary@rosemaryrodrigues.com.br

Orientador: Bruno Bottiglieri

Resumo: Este artigo tem como objetivo explorar as consequências jurídicas dos erros cometidos pelos controladores de dados em relação a eventuais confusões de dados de homônimos. Para alcançar tal compreensão, é necessário remontar uma perspectiva histórica do armazenamento de dados e a respectiva evolução do armazenamento público de dados no Brasil. Foi abordado ainda o marco regulatório da proteção de dados no país, o direito comparado e os desafios que cercam o assunto. Compreender tais assuntos é crucial para garantir a segurança jurídica e a privacidade num mundo digital em constante evolução.

Palavras chave: dados; homônimos; direito; responsabilidade civil; marco civil

THE LEGAL CONSEQUENCES OF ERRORS COMMITTED BY DATA PROCESSING AGENTS: HOMONYMS.

Abstract: This article aims to explore the legal consequences of errors made by data controllers in relation to possible homonym data mix-ups. To achieve this understanding, it is necessary to review a historical perspective of data storage and the respective evolution of public data storage in Brazil. The regulatory framework for data protection in the country, comparative law and the challenges surrounding the subject were also discussed. Understanding such matters is crucial to ensuring legal security and privacy in a constantly evolving digital world.

Keywords: data; homonyms; right; civil responsability; civil landmark

INTRODUÇÃO

Os avanços tecnológicos têm transformado radicalmente a forma como lidamos com informações e dados pessoais. Com isso, surgiram preocupações pelos operadores do direito em relação à proteção e tratamento adequado desses dados, especialmente no âmbito criminal, conforme ressaltado por Tiago Roberto Bertazo (2019):

> Certamente, uma das áreas em que o direito tem menor alcance ou dificuldade de abrangência e, consequentemente, necessita ainda mais das demais fontes

> do direito para a sua evolução é o da tecnologia. Essa afirmação decorre da grande rapidez em que a tecnologia avança; a todo momento são criadas novas soluções tecnológicas: aplicativos, redes sociais, dispositivos utilizando internet das coisas. E ainda, o mais recente uso de inteligência artificial e big data aplicados e utilizados em diversos segmentos, como, por exemplo, a captura de mais dados para serem analisados e aprendidos, pelos algoritmos de Machine Learning, servindo como base para a tomada de decisão em todos os setores da sociedade. Além disso, vale lembrar que até pouco tempo, a maior parte dos conflitos que envolvem as áreas de inovação e tecnológicas não possuíam dispositivos/normas legais próprios para promover a sua pacificação.

Nesse contexto, este artigo visa explorar as consequências jurídicas dos erros cometidos pelos agentes de tratamento de dados, com foco nos casos de homônimos, abordando também a evolução histórica do armazenamento de dados, a legislação brasileira, questões comparativas e problemáticas relacionadas a esse tema, como sugerido pelo próprio autor supracitado.

> Entende-se, portanto, que o direito conservador dos séculos passados não pertence ao jurista pós-moderno. Não obstante a criação de leis voltadas para às inovações, acredita-se que é inviável a criação demasiada de leis como forma de solução dos conflitos. Nesse sentido, espera-se que o jurista do século XXI atue de maneira técnica; remodelando velhos conceitos acadêmicos, esteja atualizado como o que ocorre na sociedade a sua volta, aplique em seus casos não só a jurisprudência, mas todas as fontes materiais e formais do direito, e o principal, desmistifique o culto do texto legal.

Assim, compreender essas questões se mostra fundamental para garantir segurança jurídica aos jurisdicionados e a privacidade dos sujeitos no mundo digital.

1. PERSPECTIVA HISTÓRICA SOBRE O ARMAZENAMENTO DE DADOS

Dados são informações ou fatos brutos que podem ser coletados, armazenados e processados. Eles representam valores, observações ou descrições de objetos, eventos ou entidades. Os dados podem ser numéricos, textuais, alfanuméricos, imagens, vídeos ou qualquer outra forma de representação digital.

Os dados por si só não possuem significado ou contexto. Eles precisam ser organizados e interpretados para obter informações úteis. A interpretação dos dados pode revelar tendências, padrões, relações de causa e efeito, ou insights valiosos para tomar decisões acertadas.

Os dados são fundamentais em diversas áreas, como ciência, negócios, tecnologia e pesquisa. Eles são coletados através de diferentes métodos, como pesquisas, sensores, medições, transações, interações digitais e muitos outros. Com o avanço da tecnologia e o crescimento exponencial das fontes de dados, como a internet e os dispositivos conectados, a quantidade e a complexidade dos dados disponíveis têm aumentado significativamente, dando origem ao termo "big data" (CETAX, 2022).

> Big Data é o termo em Tecnologia da Informação (TI) que trata sobre grandes conjuntos de dados que precisam ser processados e armazenados, o conceito do Big Data se iniciou com 3 Vs : Velocidade, Volume e Variedade. O volume de dados gerado atualmente é monstruoso, todos os dias bilhões de novas informações são geradas globalmente, pense em todos os Apps, Sistemas, TVs, Celulares, aparelhos com IoT (Internet of Things ou Internet das Coisas) que estão capturando, processando e armazenando novos dados. Cada clique que é dado em uma página ou aplicativo é automaticamente guardado para que possa ser Analisado.

Referente a perspectiva histórica do armazenamento de dados, é revelado uma trajetória de transformações significativas. Desde a antiguidade, os registros pessoais eram armazenados de forma rudimentar, em tabelas de pedra, papiros, pergaminhos e outros suportes físicos. (Silva, Momm & Benkendorf, 2018)

Com o advento da escrita, surgiram os primeiros registros organizados de dados. Posteriormente, com a invenção da imprensa, os registros passaram a ser sistematizados em documentos padronizados, como certidões e registros civis.

Antes da popularização do uso de computadores e sistemas de armazenamento eletrônico, as informações eram registradas em papel e outros meios físicos, como fotografias, filmes e documentos escritos à mão. Esses registros em papel eram armazenados em arquivos, pastas, gavetas e outros dispositivos de armazenamento físico.

Com o avanço da tecnologia, especialmente com a evolução dos computadores e sistemas de armazenamento eletrônico, muitas informações passaram a ser registradas e armazenadas digitalmente.

Hoje em dia, é comum que empresas e instituições governamentais utilizem sistemas de banco de dados para armazenar informações de clientes, usuários e cidadãos, como informações pessoais, registros de transações e outros dados relevantes.

Isso permite que as informações sejam acessadas com mais facilidade e eficiência, além de permitir a criação de backups e outras medidas de segurança para proteger as informações contra perda, roubo ou outras formas de acesso não autorizado.

Também, com o avanço tecnológico, especialmente a partir do século XX, o armazenamento de dados ganhou uma dimensão cada vez mais digital. O surgimento dos computadores e a popularização da internet permitiram a criação de bancos de dados eletrônicos, facilitando a coleta, o armazenamento e o acesso aos dados pessoais.

Não foi diferente enquanto o registro de dados dos cidadãos pelo Estado, pois, tem este o objetivo principal de garantir a correta identificação e o fornecimento dos serviços essenciais aos cidadãos, até para cumprir com suas funções sociais e constitucionais, dentre elas, a de promover a segurança e a proteção dos direitos individuais e coletivos. Existem várias razões pelas quais o Estado registra dados das pessoas:

(a). Identificação e documentação: O registro de dados permite que o Estado identifique cada indivíduo de forma única, atribuindo um número ou identificador pessoal. Isso facilita a prestação de serviços governamentais, como a emissão de documentos de identificação, registros civis (nascimento, casamento, óbito), registros fiscais, entre outros. A identificação correta e precisa é fundamental para o funcionamento adequado de várias instituições e processos governamentais.

(b). Prestação de serviços públicos: O registro de dados permite ao Estado fornecer serviços públicos essenciais, como educação, saúde, previdência social, assistência social, transporte e segurança. O conhecimento das características demográficas, socioeconômicas e de saúde dos cidadãos auxilia na elaboração de políticas públicas e na alocação eficiente de recursos.

(c) Planejamento e desenvolvimento: O registro de dados populacionais é fundamental para o planejamento e o desenvolvimento do país. As informações demográficas, como idade, sexo, localização geográfica, nível educacional e ocupação profissional, permitem ao Estado

compreender as necessidades e demandas da população, direcionar investimentos, planejar infraestruturas e serviços, e promover o desenvolvimento econômico e social de forma mais precisa e eficaz.

(d) Segurança e proteção: O registro de dados pessoais também desempenha um papel importante na segurança e proteção dos cidadãos. Ele auxilia na aplicação da lei, na prevenção e investigação de crimes, no controle de fronteiras, na gestão da segurança nacional e na proteção contra fraudes e crimes financeiros. Além disso, o registro de informações sensíveis, como grupo sanguíneo, alergias ou condições médicas, pode ser crucial em situações de emergência médica.

(e) Participação democrática: O registro de dados é relevante para a participação democrática dos cidadãos. O cadastro eleitoral, por exemplo, permite que as pessoas exerçam seu direito de voto e participem do processo político. Também pode ser utilizado para garantir a representatividade adequada em níveis governamentais, como nos censos populacionais e na delimitação de distritos eleitorais.

É importante ressaltar que o registro de dados pessoais pelo Estado deve ser realizado de forma responsável e respeitando a privacidade, a segurança e os direitos fundamentais dos indivíduos. A proteção de dados e a legislação relacionada à privacidade são aspectos fundamentais para garantir que os dados sejam usados de maneira ética e legal.

Enquanto ao modo para individualizar, as pessoas podem ser individualizadas por meio de diferentes métodos ao longo do tempo. Destacam-se alguns dos principais métodos utilizados para a individualização das pessoas:

(a) Características Físicas: Desde tempos antigos, características físicas têm sido usadas para identificar pessoas. Isso inclui traços faciais distintos, como formato do rosto, olhos, nariz, boca, entre outros. Além disso, características corporais, como altura, peso, impressões digitais e até mesmo cicatrizes ou tatuagens, podem ser utilizadas para distinguir indivíduos.

(b) Identificação Fotográfica: Com a invenção da fotografia, a identificação por meio de fotografias se tornou um método comum. As fotografias permitem a captura de

características visuais únicas de uma pessoa, como seu rosto e aparência geral. As fotos são usadas para comparar e verificar a identidade de uma pessoa.

(c) Documentos de Identificação: A emissão de documentos de identificação, como carteiras de identidade, passaportes e carteiras de motorista, também é uma maneira de individualizar as pessoas. Esses documentos contêm informações pessoais, como nome, data de nascimento, fotografia e outros dados relevantes que podem ser verificados para confirmar a identidade de alguém.

(d) Biometria: A biometria é um método de individualização que utiliza características físicas ou comportamentais exclusivas de uma pessoa. Isso inclui impressões digitais, íris, reconhecimento facial, geometria da mão, assinaturas e voz. A biometria tem se tornado cada vez mais comum em sistemas de identificação e autenticação, pois oferece uma maneira precisa e segura de verificar a identidade de alguém.

É importante observar que os métodos utilizados para individualização das pessoas evoluíram ao longo do tempo, com o avanço da tecnologia e das técnicas de identificação, à título de exemplo, trazemos as análises de DNA cada vez mais presentes, principalmente nas varas de família:

(c) DNA (Ácido Desoxirribonucleico): É uma molécula presente em todas as células vivas e contém informações genéticas que determinam as características e funções de um organismo. O DNA é composto por quatro nucleotídeos: adenina (A), citosina (C), guanina (G) e timina (T), que se ligam em pares complementares (A-T e C-G) para formar uma estrutura em dupla hélice. A sequência desses pares de bases ao longo da molécula de DNA é a responsável pelas informações genéticas que são transmitidas de geração em geração. A análise do DNA é utilizada em diversas áreas, como na investigação criminal, em exames de paternidade, em diagnósticos médicos e em estudos de biologia molecular e genética.

2. A EVOLUÇÃO DO ARMAZENAMENTO DE DADOS PÚBLICOS NO BRASIL

No Brasil, a evolução do armazenamento de dados públicos tem passado por várias transformações ao longo dos anos. Com o avanço da tecnologia da informação e a crescente

necessidade de acessar informações de forma rápida e eficiente, o armazenamento de dados públicos tem se tornado cada vez mais digitalizado e centralizado.

Anteriormente, os dados públicos no Brasil eram predominantemente armazenados em formatos físicos, como papel e microfilme. Essa forma de armazenamento apresentava diversos desafios, como a dificuldade de acessibilidade, risco de perda ou danos físicos e limitações na pesquisa e compartilhamento das informações.

Com o surgimento dos sistemas de Gerenciamento Eletrônico de Documentos (GED) e a popularização dos computadores e da internet, houve uma transição para o armazenamento digital. O governo brasileiro passou a digitalizar documentos e criar bancos de dados para facilitar o acesso e a busca por informações. Isso permitiu maior agilidade na disponibilização de dados públicos, além de contribuir para a redução de custos e a otimização dos processos de gestão documental.

Além disso, o governo brasileiro tem investido na criação de plataformas online para a disponibilização de dados públicos, como o Portal da Transparência e o e-SIC (Sistema Eletrônico do Serviço de Informações ao Cidadão). Essas iniciativas visam promover a transparência, a participação cidadã e o controle social, fornecendo acesso fácil e gratuito a informações de interesse público. (PORTAL DA TRANSPARENCIA,2023)

Nos últimos anos, o armazenamento em nuvem tem ganhado destaque no Brasil, tanto no setor público quanto no privado. A computação em nuvem oferece escalabilidade, flexibilidade e segurança para o armazenamento e o compartilhamento de dados públicos. Muitos órgãos governamentais têm adotado soluções em nuvem para garantir a disponibilidade, a integridade e a confidencialidade das informações.

No entanto, é importante destacar que a evolução do armazenamento de dados públicos no Brasil também enfrenta desafios. Dentre eles, estão a garantia da segurança da informação, a proteção da privacidade dos cidadãos, a padronização dos formatos de dados e a interoperabilidade entre os sistemas utilizados pelos diversos órgãos governamentais (ROSSO, 2019)

> A Administração Pública vem ao longo do tempo aderindo às inovações tecnológicas a ponto de se autointitular como Brasil - país digital26. Valendo-

> se de aplicativos que buscam aproximar governo e cidadão INSS, FGTS, Bolsa Família, entre outros, ou que tem como objetivo facilitar a vida da sociedade, como o e-título, a CNH Digital, o Meu Imposto de Renda, está entre os maiores controladores de dados do país. Diante destes fatos, nos chamou atenção o pouco interesse que o setor público demonstrou ao não participar dos debates que antecederam a aprovação da Lei Geral de Proteção de Dados bem como a posterior tentativa de colocar-se fora de seu alcance demonstrado o quão despreparadas estão as entidades públicas diante da nova lei.
>
> Devemos fazer menção ao fato de que existem muitos pontos obscuros e que deverão pautar as discussões durante e mesmo após a implementação das regras de conformidade no setor público, entretanto, parece-nos que tal como o que recentemente ocorreu nos países europeus na implantação do GDPR, a administração pública tem andado a passos lentos quando se trata de adequação à lei. Conforme apresentamos no texto, são vários os aplicativos que coletam dados desnecessários para o seu funcionamento, ou seja, não se adota a minimização da coleta, também não se verifica nos diversos sistemas existentes explicações sobre a finalidade específica para qual o dado é coletado.

Em resumo, a evolução do armazenamento de dados públicos no Brasil tem acompanhado as tendências tecnológicas, passando de formatos físicos para soluções digitais, como os sistemas de gerenciamento eletrônico de documentos e as plataformas online. A computação em nuvem tem se destacado como uma opção viável e segura para o armazenamento e compartilhamento de dados públicos, promovendo a transparência e a eficiência na gestão pública, no entanto e, como dito anteriormente, ainda há desafios a serem superados para garantir a segurança, a privacidade e a interoperabilidade dos dados.

3. O MARCO REGULATÓRIO DOS DADOS NO BRASIL

O Marco Regulatório dos Dados no Brasil refere-se a um conjunto de leis e regulamentações relacionadas à proteção de dados pessoais e à governança de dados no país. O principal componente desse marco regulatório é a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que foi aprovada em agosto de 2018 e entrou em vigor em setembro de 2020.

A Lei Geral de Proteção de Dados (LGPD) foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e tem como objetivo principal proteger os direitos das pessoas em relação ao tratamento de seus dados pessoais. Algumas características marcantes do instituto no Brasil incluem:

(a) Consentimento: As empresas que coletam e processam dados pessoais devem obter o consentimento claro e explícito dos titulares dos dados. As pessoas têm o direito de revogar esse consentimento a qualquer momento.

(b) Direitos dos titulares: A LGPD concede aos titulares dos dados diversos direitos, incluindo o direito de acessar seus dados, corrigi-los, excluí-los e solicitar a portabilidade dos mesmos.

(c) Responsabilidade das empresas: As organizações que lidam com dados pessoais devem adotar medidas de segurança adequadas para proteger essas informações. Elas também são obrigadas a nomear um Encarregado de Proteção de Dados (DPO) e notificar as autoridades e os titulares dos dados em caso de violações de segurança.

(d) Transferência internacional de dados: A LGPD regula a transferência de dados pessoais para países que não têm um nível adequado de proteção de dados, exigindo garantias de segurança, como cláusulas contratuais ou normas corporativas globais.

(e) Fiscalização e penalidades: A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade responsável por fiscalizar o cumprimento da LGPD. Empresas que não cumprem as disposições da lei podem estar sujeitas a multas e outras sanções.

A Lei Geral de Proteção de Dados (LGPD) ainda possui o Capítulo IV, ao qual dedica-se ao tema "Tratamento de Dados Pessoais pelo Setor Público" e indica que a integração com à Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011), a qual prescreve em seu artigo 23:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

Outrossim, a Lei de Acesso à Informação dispõe que:

> Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
>
> I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
>
> II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e
>
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

4. AS PROBLEMÁTICAS QUANTO AO TRATAMENTO E ARMAZENAMENTO DE DADOS

O tratamento e armazenamento de dados são questões críticas em nossa sociedade cada vez mais digital e interconectada. Existem várias problemáticas associadas a esses processos, dentre eles, destacamos:

(a) Privacidade e Segurança: Uma das maiores preocupações é a violação da privacidade. Muitas empresas coletam uma grande quantidade de dados pessoais dos usuários, e isso pode ser explorado de maneira indevida se não houver medidas de segurança adequadas. Vazamentos de dados e breaches de segurança são cada vez mais comuns, o que pode resultar em danos financeiros e à reputação das empresas, além de impactar negativamente os indivíduos cujos dados foram comprometidos.

(b) Uso Indevido de Dados: Os dados coletados podem ser usados de maneira indevida, seja para fins de publicidade direcionada, discriminação, manipulação política, ou mesmo fraudes. O uso inadequado de informações pessoais pode ter sérias consequências para a sociedade.

(c) Falhas de Consentimento: Nem sempre os indivíduos estão cientes do que estão consentindo ao compartilhar seus dados. Políticas de privacidade muitas vezes são longas e de difícil compreensão. Isso levanta questões sobre a validade do consentimento e se as pessoas realmente compreendem como seus dados serão usados.

(d) Vieses e Discriminação: Algoritmos de aprendizado de máquina que tomam decisões com base em dados podem perpetuar preconceitos existentes nos dados de treinamento, resultando em discriminação em várias áreas, como emprego, crédito e justiça.

(e) Armazenamento Excessivo: Algumas organizações armazenam dados por tempo indeterminado, o que não apenas representa riscos de segurança, mas também levanta preocupações éticas sobre a necessidade real de reter informações pessoais por tanto tempo.

(f) Desafios Legais e Regulatórios: As leis e regulamentos sobre tratamento e armazenamento de dados estão em constante evolução e podem variar de país para país. Isso pode criar complexidade e desafios para as organizações que operam globalmente.

(g) Custos e Escala: Com a crescente quantidade de dados gerados a cada dia, o armazenamento e processamento de dados em larga escala tornam-se caros e complexos.

(h) Transparência e Responsabilidade: Muitas vezes, é difícil para os indivíduos rastrearem como suas informações são usadas e por quem. Isso gera uma falta de transparência e torna a responsabilização das organizações mais desafiadora.

Para abordar essas problemáticas, muitos países implementaram leis de proteção de dados, como o GDPR na União Europeia e a LGPD no Brasil, que estabelecem diretrizes rigorosas para o tratamento de dados pessoais.

> A dependência absoluta em utilizar esses dados como insumo da economia, o potencial lucrativo, o surgimento de novos mecanismos de tratamento e de novos modelos de negócios até então sequer imaginados, o assustador volume produzido em cada segundo - que denominamos big data - as conclusões que podemos chegar a partir da sua análise para as mais diversas áreas fez com que a União Europeia, que desde 1995 já tinha a sua política de proteção de dados, edita-se um novo regulamento - o GDPR1 - muito mais completo e abrangente, com modalidades de penalizações severas No Brasil não foi diferente, embora com um tanto mais de morosidade legislativa, em 20, após quase uma década de discussões, por fim foi criada a Lei Geral de Proteção de Dados - LGPD. (ROSSO, 2019)

Além disso, as organizações estão investindo em práticas de segurança de dados mais robustas e em maior transparência em relação ao uso de informações pessoais.

O debate sobre como equilibrar a inovação tecnológica com a proteção da privacidade e a justiça continua a evoluir à medida que enfrentamos esses desafios em um mundo cada vez mais digital.

5. PESQUISAS INCOMPLETAS E CONFUSÃO DE HOMÔNIMOS NO ÂMBITO DA JUSTIÇA CRIMINAL

A pesquisa incompleta e a confusão de homônimos, principalmente em âmbito criminal, são questões importantes no sistema legal que podem ter sérias consequências para a justiça e os direitos individuais.

Com relação às pesquisas incompletas, também conhecidas como pesquisas inadequadas, é aquela que não reúne todas as evidências necessárias para estabelecer a verdade nos processos criminais. Isso pode acontecer por diversas razões:

(a) Falta de recursos, onde agentes policiais, com recursos limitados para investigar crimes, realiza investigações superficiais que não coletam todas as evidências relevantes de autoria.

(b) Erro humano, onde investigadores podem cometer erros ao coletar, preservar ou analisar evidências. Isso pode incluir a perda de provas, a contaminação de evidências ou o depoimento incorreto de testemunhas.

(c) Vieses: Investigadores podem ser influenciados por vieses conscientes ou inconscientes que afetam a forma como conduzem a pesquisa, por exemplo, o racismo estrutural, qual acarreta à focalização injusta em determinados suspeitos ou teorias.

Destarte, o compartilhamento ou armazenamento equivocado de dados entre o serviço público e o privado podem resultar em condenações injustas de pessoas inocentes ou na absolvição de culpados.

A confusão em relação aos homônimos é outro problema que pode se manifestar, principalmente, no sistema de justiça criminal. Isso acontece quando duas ou mais pessoas têm nomes idênticos ou muito semelhantes, o que pode levar a erros de identificação e acusações equivocadas (como por exemplo, José da Silva ou Maria da Silva).

(d) Registros criminais compartilhados: Se duas pessoas com nomes semelhantes têm registros criminais, é possível que as acusações ou condenações de uma pessoa sejam erroneamente associadas à outra.

(e) Identificação inadequada: Testemunhas oculares ou vítimas podem identificar erroneamente uma pessoa com base apenas em um nome semelhante, ignorando outras características distintivas.

(f) Processo legal injusto: A confusão de homônimos pode levar a acusações injustas e processos judiciais para pessoas que não cometeram crimes.

Para evitar a confusão de homônimos, é essencial que os sistemas judiciais utilizem procedimentos rigorosos de verificação de identidade, incluindo impressões digitais, fotografias e outras informações biométricas quando disponíveis. Além disso, os advogados de defesa devem estar atentos a essa possibilidade e buscar esclarecimentos quando a identidade do réu estiver em questão.

Portanto, pesquisas incompletas e confusão de homônimos são problemas reais no âmbito criminal que podem resultar em injustiças. Para garantir a justiça e a integridade do sistema legal, é fundamental que as investigações sejam conduzidas de forma completa e imparcial, e que medidas adequadas sejam tomadas para evitar a confusão de homônimos durante o processo criminal.

6. CASOS DE PRESOS POR HOMÔNIMOS E RESULTADOS DE JULGAMENTOS.

Casos de pessoas sendo presas devido a homônimos são exemplos de erros judiciais que podem ter consequências devastadoras para os indivíduos envolvidos e destacam as fragilidades do sistema de justiça.

Quando duas ou mais pessoas compartilham nomes idênticos ou muito semelhantes, existe o risco de confusão, resultando em prisões, acusações e julgamentos equivocados. Registre-se que tais casos são rotineiros, embora ignorados por parte dos operadores do direito, como evidenciado abaixo, à titulo de exemplo, relato do próprio portal de notícias do Tribunal de Justiça de Minas Gerais:

> A 3ª Câmara Cível do Tribunal de Justiça de Minas Gerais manteve sentença da Comarca de Belo Horizonte que condenou o Estado de Minas Gerais a indenizar um funcionário público em R$ 6 mil por danos materiais e em R$ 15 mil por danos morais por tê-lo prendido de forma equivocada por suspeita de ter cometido crime.
>
> Durante uma blitz de trânsito em 3 de outubro de 2017, o servidor, que é engenheiro e estava de viagem com a esposa, foi preso por policiais militares. A alegação foi de que havia um mandado de prisão em aberto contra o homem, expedido na Comarca de Araçuaí devido a um estupro de vulnerável, ocorrido no município de Coronel Murta.
>
> O servidor foi levado à delegacia e mantido preso em uma cela, enquanto a autoridade policial verificou com a delegacia de Araçuaí que se tratava de um homônimo do criminoso e que de havia ocorrido um engano.
>
> O servidor público afirma que mora em Belo Horizonte e o crime foi cometido em uma cidade a mais de 560 quilômetros da capital, onde ele nunca esteve. Diante disso, sustentou que, além da humilhação, foi obrigado a contratar advogado para livrá-lo da prisão e teve prejuízo financeiro, o que levou-o a ajuizar a ação com pedido de indenização pelos danos. (TJMG, 2023)

No Tribunal de Justiça da Paraíba:

> A Primeira Câmara Cível do Tribunal de Justiça da Paraíba manteve a sentença na qual o Estado da Paraíba foi condenado a pagar a quantia de R$ 40 mil, a título de danos morais, decorrente da prisão de um homem por ser homônimo de réu em processo penal em trâmite no 1º Tribunal do Júri da Capital.
>
> No processo, a parte autora alega que no dia 16 de fevereiro de 2017 estava em sua academia, quando foi abordado por policiais civis que realizaram sua prisão em razão de mandado de prisão expedido por Vara criminal da Capital em razão da prática de crimes de homicídio tentado e consumado. Narra, ainda, que somente foi colocado em liberdade no dia 17 de fevereiro de 2017, por ocasião de audiência de custódia, pelo Juizo do 1º Tribunal do Júri, após pedido da defesa e do Ministério Público, em razão da homonímia. (TJPB, 2021)

No Tribunal de Justiça de Santa Catarina:

> O juízo da 2ª Vara Cível da comarca de Navegantes condenou o Estado de Santa Catarina ao pagamento de R$ 30 mil, por danos morais, a um homem que foi preso por engano. Ele tinha o mesmo nome de um réu condenado pelos crimes de homicídio e roubo em outro Estado, foi preso em 16 de abril de 2017 e permaneceu mais de um mês encarcerado equivocadamente.

> Consta nos autos que o autor da ação, naquela data, estava em sua residência quando foi preso erroneamente por policiais em cumprimento de mandado de prisão expedido pela Vara de Execuções Penais de Belém, no Pará. Ele teria tentado esclarecer a questão no momento da prisão, sem sucesso. O homem foi colocado em liberdade após 35 dias de cárcere, 11 deles em total isolamento. Para reforçar seu pleito indenizatório, sustentou também ser portador de diabetes e não ter recebido alimentação e medicação adequadas no período em que ficou atrás das grades. (TJSC, 2021)

No Tribunal de Justiça do Distrito Federal:

> A 2ª Turma Recursal dos Juizados Especiais do DF manteve a decisão que condenou o Distrito Federal a indenizar um homem que foi submetido à prisão civil indevida. Os julgadores entenderam que a detenção de alguém por erro do Estado determina a ocorrência de dano moral indenizável.
>
> Consta nos autos que, em 05 de dezembro, o autor foi encaminhado para a 15ª Delegacia de Ceilândia sob o argumento de que havia mandado de prisão civil aberto em seu desfavor expedido pela Vara de Família e Sucessões de Jaguapitã, no Paraná. Ao chegar à delegacia, no entanto, esclareceu que nunca morou na cidade paranaense e que não tinha filhos fora do DF. Ele relata ainda que só foi solto dia 11 de dezembro após ser constatada a homonímia.
>
> Decisão do 1º Juizado Especial da Fazenda Pública do DF condenou o DF a pagar ao autor a quantia de R$ 15 mil a título de indenização dos danos morais. (TJDF, 2020)

No Tribunal de Justiça da Bahia:

> O drama vivido na Justiça pelo lavador de carro Edmilson da Conceição (39), teve um fim na noite desta última quinta-feira (11), em Salvador, Bahia. Identificado como criminoso por ter o mesmo nome de um homem condenado por um roubo de R$ 440, em outro município baiano, Edmilson completaria hoje (12) nove meses de reclusão em uma unidade prisional na Bahia. Em uma infeliz coincidência, sua mãe, a doméstica Maria Isabel da Conceição (57), também é homônima da mãe do condenado, o que agravou ainda mais o equívoco. O Edmilson que cometeu verdadeiramente o roubo está foragido e já teve sua prisão decretada.
>
> Morador do bairro de Tancredo Neves, periferia de Salvador, casado e pai de duas filhas, Edmilson, o inocente, conta que foi preso por engano durante o Carnaval desse ano, quando brincava ao lado de sua irmã e amigos. Pego de surpresa com coronhadas na cabeça dada por policiais, ele foi levado à Delegacia, onde foi constatado, erradamente, que se tratava do homem que havia roubado uma quantia de R$40 em dinheiro e um cheque de R$ 400, no município de Itanagra, interior do Estado.

> Depois de passar nove meses na Cadeia Pública de Salvador, onde, segundo ele, sofreu espancamento e várias outras formas de agressão, somente agora Edmilson pôde ter sua inocência comprovada, após atuação da Central de Atendimento a Presos em Delegacia - Capred, da Defensoria Pública do Estado, que identificou o erro, realizou testes de impressão digital e deu procedeu com com um pedido de relaxamento de prisão, ao qual o lavador tinha direito. O pedido resultou em um alvará de soltura em favor de Edmilson, expedido pelo juiz da comarca de Mata de São João, distante a 94km da capital, Admar Ferreira Souza, o mesmo que havia decretado a prisão. As denúncias de espancamento estão sendo investigadas pela Defensoria Pública. (DPEBA, 2010)

Assim, podemos delimitar como as principais causas na confusão de homônimos:

(a) Registro civil idêntico: Quando pessoas com nomes homônimos têm registros de nascimento semelhantes ou idênticos, é fácil para as autoridades confundirem as identidades.

(b) Falta de informações detalhadas: Em alguns casos, a falta de informações adicionais, como data de nascimento, endereço ou número de identificação pessoal, torna difícil para as autoridades distinguirem entre indivíduos com nomes semelhantes.

(c) Erros de processamento de dados: Erros na inserção de informações nos sistemas de justiça podem resultar na associação equivocada de registros criminais a pessoas com nomes semelhantes.

(d) Identificação inadequada: Testemunhas oculares ou vítimas podem identificar erroneamente uma pessoa com base apenas em um nome semelhante, ignorando outras características distintivas.

7. MEDIDAS PREVENTIVAS

Para prevenir casos de prisões injustas por homônimos e corrigir equívocos quando eles ocorrem, é crucial implementar medidas adequadas, tais como:

(a) Verificação rigorosa de identidade: As autoridades judiciais devem realizar verificações detalhadas de identidade, incluindo impressões digitais, fotografias e outras informações biométricas, quando disponíveis.

(b) Compartilhamento de informações: Bancos de dados policiais e de justiça devem ser projetados para minimizar a confusão de homônimos, garantindo que outras informações distintivas sejam incluídas nos registros.

(c) Treinamento de pessoal: Treinar investigadores, advogados e juízes sobre a importância de distinguir entre homônimos e a necessidade de evidências sólidas é fundamental para evitar erros judiciais.

(d) Revisão de casos: Os sistemas legais devem ter procedimentos eficazes de revisão de casos para identificar e corrigir erros judiciais quando a confusão de homônimos é descoberta.

Resumindo, casos de prisão devido a homônimos deve ser assimilado como uma preocupação legítima no sistema de justiça e tem condão de resultar em inúmeras condenações injustas, destarte, para evitar esses erros, é fundamental adotar medidas que garantam uma identificação precisa e uma revisão rigorosa dos casos, para garantir que a justiça seja verdadeiramente servida e que indivíduos inocentes não sejam prejudicados por erros de identificação.

8. MEDIDAS REPRESSIVAS

A incorreções de dados podem sugerir intervenção e tutela jurisdicional ou, quando ocorrida pelo próprio sistema de justiça, necessária as devidas correções e reparações no intuito de para proteger os direitos dos indivíduos e a manutenção da confiança social nos sistemas públicos. Destarte, percebe-se que uma confusão de homônimo pode sugerir:

(a) Revisão de Casos: Um dos primeiros passos para corrigir um erro judicial é a revisão completa do caso. Isso pode envolver a análise de novas evidências, revisão das decisões anteriores e avaliação de qualquer procedimento inadequado.

(b) Liberação de Inocentes: Se ficar claro que um réu foi condenado injustamente, medidas devem ser tomadas para sua liberação imediata e compensação pelos anos de prisão injustos.

(c) Reabertura de Casos: Em alguns casos, um erro judicial pode levar à reabertura do processo legal para permitir que novas evidências sejam consideradas ou que um novo julgamento seja realizado.

(d) Reforma Legal: Erros judiciais frequentes podem destacar a necessidade de reformas legais para melhorar os processos judiciais, incluindo a coleta e a apresentação de evidências.

(e) Responsabilização: Quando erros judiciais resultam de má conduta de agentes da lei, é importante que haja responsabilização por suas ações, que podem incluir ações disciplinares ou processos criminais.

(f) Reparação: Além de liberar os inocentes, o sistema legal deve considerar medidas de reparação, como compensação financeira, assistência à reintegração e apoio psicológico para aqueles que foram prejudicados por erros judiciais.

Entende-se como fundamental que, quando esses erros sejam identificados, medidas corretivas e preventivas eficazes sejam tomadas para garantir a justiça e a integridade do sistema de justiça. A revisão de casos, a liberação de inocentes e a responsabilização por má conduta são passos cruciais para garantir que o sistema legal funcione de maneira justa e equitativa.

9. CONCLUSÃO

No cenário atual, onde a tecnologia desempenha um papel central em nossas vidas, a proteção de dados pessoais é mais crítica do que nunca. A análise das consequências jurídicas dos erros cometidos pelos agentes de tratamento de dados, especialmente em casos de homônimos no âmbito criminal, demonstra a importância de uma legislação sólida e abordagens cuidadosas no armazenamento e tratamento de informações. A perspectiva histórica nos mostra como chegamos a esse ponto, enquanto a análise do direito comparado revela diferentes abordagens em todo o mundo.

O marco regulatório dos dados no Brasil representa um avanço significativo na proteção da privacidade, mas também revela desafios complexos. As problemáticas identificadas

destacam a necessidade contínua de adaptação às mudanças tecnológicas e ameaças à segurança de dados.

Concluímos, então, que a questão das consequências jurídicas relacionadas a erros no tratamento de dados é multifacetada e está em constante evolução. É imperativo que governos, empresas e sociedade civil continuem a colaborar para desenvolver soluções que equilibrem a inovação tecnológica com a proteção dos direitos individuais e a justiça no âmbito criminal.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

COMPARATO, Fábio Konder. A afirmação histórica dos direitos humanos. 11. ed. São Paulo: Saraiva, 2015.

FERRAZ JUNIOR, Tércio Sampaio. Introdução ao Estudo do Direito: técnica, decisão, dominação. 6. ed. São Paulo: Atlas, 2016.

GARCIA, Emerson. Proteção de dados pessoais no Brasil: comentários à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). São Paulo: Revista dos Tribunais, 2019.

Health Insurance Portability and Accountability Act (HIPAA) dos Estados Unidos.

MACHADO, Marta Watanabe. Proteção de dados pessoais e o princípio da autodeterminação informativa. São Paulo: Saraiva Educação, 2019.

POZZOBON, Carolina. Tratamento de dados pessoais sensíveis: uma análise à luz da Lei Geral de Proteção de Dados Pessoais. Porto Alegre: Atlas, 2019.

Privacy Act dos Estados Unidos.

REGO, Thiago Marrara. O direito ao esquecimento no Brasil: uma análise à luz da Lei Geral de Proteção de Dados Pessoais. Rio de Janeiro: Lumen Juris, 2020.

Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia.

ROCHA, Gabriel. A proteção de dados pessoais e a Lei Geral de Proteção de Dados: comentários à Lei nº 13.709/2018. São Paulo: Atlas, 2019.

SARLET, Ingo Wolfgang. Direitos fundamentais e direito privado. 12. ed. Porto Alegre: Livraria do Advogado, 2016.

SILVA, Rafael Zanatta da. Proteção de dados pessoais no Brasil: comentários à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Porto Alegre: Sérgio Antônio Fabris Editor, 2018.

https://www.migalhas.com.br/depeso/290669/direito-e-tecnologia--a-diferenca-oceanica-existente-entre-os-avancos-tecnologicos-e-a-regulamentacao-juridica
https://cetax.com.br/big-data/

https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=35640
https://www.gov.br/abin/pt-br/acesso-a-informacao/servico-de-informacao-ao-cidadao

https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios

https://www.tjmg.jus.br/portal-tjmg/noticias/homem-preso-ao-ser-confundido-com-homonimo-sera-indenizado-8ACC80C2890F39DF01894BE92AAD7267.htm

https://www.tjpb.jus.br/noticia/homem-preso-no-lugar-de-homonimo-sera-indenizado-em-r-40-mil

https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/setembro/distrito-federal-deve-indenizar-homem-submetido-a-prisao-civil-indevida

https://www.defensoria.ba.def.br/noticias/inocente-homonimo-de-acusado-e-solto-apos-atuacao-da-defensoria-publica/