UNiSA Universidade de Santo Amaro

Pluralistas

Proteção de Dados: criptografia de segurança em conflito com a publicidade dentro de decisões do STF.

Lucas Buonanato Barros [3]

Victor Pegoraro [2]

Resumo

A criptografia de dados em síntese é uma ferramenta para proteger a privacidade e a segurança de uma informação pessoal ou sensível. Podendo em diversos casos entrar diretamente me conflito com o princípio da publicidade, que norteia em direção a transparência e acessibilidade das informações. Pois, a criptografia limita o acesso a dados, assim quando observamos as decisões dentro do STF, o princípio da publicidade é latente em virtude do impacto social de suas decisões, todavia, quando as informações estão disponíveis indiscriminadamente, podem ocasionar graves consequências para aqueles que têm essas informações disponibilizadas.

Desta maneira entender a criptografia e como ela atua dentro das decisões do supremo tribunal federal, sendo ferramenta útil para atender toda a demanda do judiciário e da segurança que ele necessita, se mostra pedra basilar no cenário contemporâneo diante da crescente dependência de dados digitais na administração pública e na prestação de serviços.

Palavras-chaves: Criptografia; Dados; Decisões; STF.

Abstract

Data encryption is a primary tool for protecting the privacy and security of personal information. However, this technology may conflict with the principle of publicity, which values transparency and accessibility of information. Encryption limits access to data, so when we observe the decisions within the STF, the principle of publicity is latent due to the social impact of its decisions, however, when information is available indiscriminately, it can cause serious consequences for those who have this information available.

In this way, understanding encryption data, and how it applied within the decisions of the supreme court, being a useful tool to understand the demands of the judiciary and the security in encryption that it needs, is a pillar in the contemporary scenario in the face of the growing dependence on digital data in public administration.

Keywords: Encryption; Data; Decisions; STF.

[1] Graduando em Direito, Universidade de Santo Amaro

[2] Orientador

Introdução

O presente trabalho de conclusão de curso, apresentado em forma de artigo, tem como meta norteadora entender a proteção de dados dentro das decisões do STF e como elas podem ditar o comportamento do judiciário, visto a utilização de ferramentas para invasões de sistemas e utilização de informações de forma indevida, para além do aumento significativo de vazamentos de dados pessoais sensíveis, utilizando como método de proteção a criptografia, visando manter o equilíbrio de proteção com publicidade, e como a criptografia pode dirimir esse conflito sem deixar de lado a participação social.

Nessa análise, buscamos critérios objetivos para propor soluções validadas, visto que a proteção de dados é um dos temas mais debatidos, especialmente diante do avanço tecnológico e do aumento exponencial do uso de informações digitais. A criptografia de segurança é ferramenta crucial para garantir a confidencialidade e a integridade dos dados, garantindo a transparência a liberdade de expressão. Todavia, seu uso restritivo pode entrar em conflito com o princípio da publicidade, que visa a transparência e principalmente o acesso às informações, especialmente dentro do judiciário.

Tendo como objetivo geral, analisar o impacto do uso da criptografia como mecanismo de proteção de dados nas decisões do Supremo Tribunal Federal (STF), investigando os possíveis conflitos com o princípio da publicidade e propondo soluções que equilibrem segurança e transparência. Bem como objetivo específico, identificar os fundamentos jurídicos do princípio da publicidade e históricos da proteção de dados no contexto brasileiro; estudar a aplicação da criptografia como ferramenta de segurança da informação, verificados os métodos mais utilizados das ferramentas e o tratamento de dados sensíveis; investigar como outros países lidam com a relação entre segurança de dados e publicidade nos tribunais; analisar o conflito proposto e as medidas possíveis para saneamento do conflito no contexto das decisões do STF.

Conceitos

1.1 Breve histórico

Diante do exposto supra, para melhor entendermos o conflito que será debatido, faz-se necessário a conceitualização de criptografia e sua evolução histórica, destarte, a criptografia é uma ferramenta essencial para proteger a comunicação e principalmente a informação ao longo da evolução humana, feito através da mudança da informação para uma versão que não pode ser acessada por todos, sendo acessada apenas pelo destinatário dela.

Assim, como no império romano, onde ocorreu a cifra de César, que consistia em um simples deslocamento de letras no alfabeto, visando a confusão da mensagem perante o inimigo.

Com o tempo, métodos mais sofisticados surgiram, como a cifra de *Vigenère*, que dificultava a decodificação, sendo por sua vez, a primeira a introduzir uma chave variável, necessária pa-

ra entender a mensagem, fato esse muito utilizado posteriormente em decodificações mais modernas, usando criptografia para garantir a segurança de documentos e mensagens estratégicas.

Quando adentramos o século XX, a criptografia ganhou destaque na Segunda Guerra Mundial com o uso da máquina Enigma pelos alemães, que utilizava para seu funcionamento, cilindros e engrenagens de forma complexa para transmissão da informação, todavia, esforços de cientistas e matemáticos, como Alan Turing, levaram à quebra de seu código, direcionando posteriormente as matrizes do que viria a ser a evolução da computação.

A partir da década de 60 dados pessoais e informações ganharam contornos diferentes em virtude das relações privadas e do entendimento social sobre as informações pessoais e de dados, conforme disposto nas palavras do professor Machado da UFRJ:

> A partir da década de 1960, o conceito de informação pessoal passou de algo que era meramente pressuposto (pois a garantia da privacidade deveria necessariamente compreender a proteção dos documentos e informações de natureza privada) para gradativamente emergir como conceito central para a tutela jurídica da privacidade. Isso tem direta correspondência com a transformação do sentido social de privacidade a que Stefano Rodotà faz alusão: de um sentido negativo, de confidencialidade e reserva sobre a esfera privada – logo, atinente a dados necessariamente vinculados ao indivíduo e suas relações particulares –, para compreender o controle dinâmico sobre as próprias informações. (MACHADO, Diego; DONEDA, Danilo, 2018, p.103).

Destarte, com a miniaturização dos chipsets e computadores caseiros, deu-se início a evolução da criptografia computacional, fazendo-se necessária a segurança digital com as informações pessoais transmitidas, principalmente pela internet, deixando-as seguras e confiáveis.

1.2 Conceito de criptografia

A criptografia de forma resumida, refere-se à transformação de informações de um formato compreensível para um formato codificado. Esses dados codificados só podem ser acessados após serem interpretados para um formato legível, conforme delimitado pelo professor da USP, Prof. Dr. Terada:

> Algoritmos criptográficos basicamente objetificam "esconder" informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia. (TERADA, Routo, 2011, p.18).

Assim, a criptografia é o componente essencial para a proteção de informações que se deseja manter protegida. Visando assim, assegurar que os dados de um sistema computacional não sejam apropriados ou visualizados por indivíduos com intenções maliciosas, como a obtenção de

dados pessoais sensíveis.

Destarte, dados pessoais sensíveis são aqueles identificados para aquele determinado indivíduo, podendo ser utilizados para diversos fins diferentes daqueles aos quais foram disponibilizados, como vemos nas palavras do Prof. Machado da UFRJ:

> Na conceitualização restrita, por dado pessoal entende-se a representação de fatos sobre pessoa identificada, isto é, representação referente a alguém que se conhece e individualiza em meio a certo grupo ou coletividade. O processo de identificação aí operado é possível a partir de elementos informativos chamados identificadores, os quais mantém relação particularmente privilegiada e próxima com certo indivíduo. (MACHADO, Diego; DONEDA, Danilo, 2018, p. 105).

Para tanto, visando protegê-los, são utilizados programas de criptografia de dados, também chamados de algoritmos de codificação e encriptação, projetados para criar um sistema de codificação.

1.3 Como funciona

Ao compartilhar informações ou dados, eles percorrem uma rede de dispositivos conectados que integram a Internet pública. Durante este trânsito pela Internet, existe o risco de que os dados sejam comprometidos ou apropriados. Para mitigar esses perigos, deve-se adotar programas especializados para assegurar que as informações sejam transmitidas de forma segura, conhecidos como criptografia para proteção em redes, protegendo os dados sensíveis, sendo esses dados entendidos como:

> Os dados não apresentam significado de relevância e nem compreensão sozinhos, não tem sentido a princípio, e por isso não tem valor algum. Já a informação consiste na ordenação e a organização dos dados de maneira a fazer sentido, abrangendo um significado que dê respaldo ao conhecimento, sendo, portanto, sensíveis. (RICHTER, Alexandre L., 2025, p. 5).

A criptografia consiste na transformação de texto compreensível em uma versão indecifrável, cifrando esse texto. Tratando de modificar dados claros para que se apresentem de maneira aparentemente aleatória aos olhos daquele que não é o destinatário principal da informação. Por sua vez, esse processo utiliza uma chave criptográfica, que é um conjunto de valores matemáticos previamente acordados entre o emissor e o receptor. O receptor aplica a chave para decodificar os dados, retornando-os ao formato original, em texto legível.

> O processo de criptografia envolve a execução de um algoritmo que faça a codificação dos dados para que se tornem irreconhecíveis, sendo necessário um algoritmo para descriptografar estes dados utilizando-se uma chave específica (RICHTER,Alexandre L., 2025, p. 5).

Cumpre salientar, que quanto maior for a complexidade da chave criptográfica, por sua vez maior será a eficiência da proteção da informação pretendida, pois torna-se mais difícil para terceiros decifrarem os dados utilizando técnicas de força bruta, que consistem em testar combinações aleatórias até identificar a correta.

1.4 Técnicas e protocolos de criptografia comumente aplicados

Para tanto, temos que a utilização se dá por diferentes métodos, primeiro os dois métodos de criptografia mais utilizados são o simétrico e o assimétrico, utilizando como analogia um cadeado e a utilização de chaves para sua abertura, assim o termo se referem à utilização ou não da mesma chave para codificar e decodificar os dados.

Na criptografia simétrica, também chamada de criptografia de chave privada, emprega-se uma única chave para realizar tanto a encriptação quanto a decriptação, ou na analogia do cadeado, a mesma chave "tranca" e a mesma que "abre", na sendo essa modalidade ideal para usuários individuais e sistemas fechados, visto que não necessariamente existe a necessidade do envio da chave. Se houver a necessidade de enviar a chave ao destinatário, isso pode aumentar a vulnerabilidade ao risco de interceptação por terceiros, como hackers. Para além disso, ele apresenta uma velocidade superior de criptografia em comparação com a criptografia assimétrica.

Por outro lado, a criptografia assimétrica utiliza duas chaves distintas, sendo uma pública e outra privada, matematicamente interligadas. Destarte, essas chaves são grandes números emparelhados, mas não idênticos, o que justifica o termo "assimétrico".

> Utiliza-se a encriptação assimétrica para cifrar dados pequenos, sendo que seu principal uso é a assinatura digital e na realização de troca de chaves de maneira segura. [...]. Já a encriptação simétrica é usada na ocultação de conteúdo dos blocos ou fluxo contínuo de dados de qualquer tamanho [...]. (RICHTER,Alexandre L., 2025, p. 5)

A chave privada permanece em sigilo com o usuário, enquanto a chave pública pode ser distribuída a destinatários autorizados ou disponibilizada amplamente. Assim, as informações encriptadas com a chave pública do destinatário só podem ser revertidas ao seu formato original por meio da chave privada correspondente.

1.4.1 - Exemplos de algoritmos de criptografia

Os métodos de criptografia são desenvolvidos para converter dados ou informações em código cifrado ilegível. Cada algoritmo utiliza uma chave de encriptação para modificar os dados utilizando para tanto, ferramentas matemáticas, de modo que, embora o conteúdo cifrado pareça aleatório, ele possa ser revertido ao texto original por meio da aplicação da chave da chave de decodificação correta.

Segundo o Professor Ph.D. Routo Terada (2011),, do departamento de ciências da computação da USP, em seu livro Segurança de dados: criptografia em rede de computadores, existem várias categorias criptografia, sendo subjetivamente cada uma utilizada para atender a alguns objetivos específicos, sendo substituídas assim que suas vulnerabilidades são conhecidas, entre os algoritmos de criptografia mais conhecidos, estão:

Assim temos a criptografia D.E.S (Data Encryption Standard.), subjetividade um dos mais importantes avanços na criptografia moderna, que basicamente consiste em um algoritmo simétrico concebido na década de 70, que durante muitos anos serviu como um padrão de segurança nos Estados Unidos. Sendo sua criptografia por blocos, através de diversos processos matemáticos, convertendo os dados em grupos de 64 bits ao longo de 16 ciclos que incluem substituição e transposição. Esse método é considerado ultrapassado, todavia é a base para as futuras ferramentas de criptografia.

Passamos para a criptografia 3.D.E.S: Também conhecido como *Triple Data Encryption Standard*, o 3.D.E.S é um algoritmo simétrico que realiza a encriptação dos dados basicamente passando pelos mesmos processos que o desenvolvido pela ferramenta DES, porém três vezes. Um sistema confiável por sua robustez, sendo um recurso amplamente confiável em implementações de hardware, especialmente no setor financeiro.

Temos também a criptografia A.E.S ou *Advanced Encryption Standard*, desenvolvido para aprimorar e substituir o DES original, por isso o termo avançado empregado no nome. Esse algoritmo é amplamente aplicado, principalmente em programas de mensagens, como WhatsApp, sendo divulgado assim com a utilização de outros processos de "criptografia de ponta a ponta", além de ser utilizado em ferramentas de compactação, como o WinZip.

Por sua vez temos a criptografia RSA que o primeiro algoritmo de criptografia assimétrica a ser disponibilizado em larga escala ao público. Muito popular devido a tamanho robusto das chaves que emprega, o que o torna essencial para a transmissão segura de informações utilizando um par de chaves distintas para a encriptação e decriptação dos dados.

Além desses métodos de encriptação, há também aqueles designados como *Common Criteria* (CC), esse por si só não é um padrão de encriptação, mas sim um conjunto de diretrizes internacionais destinadas a avaliar os requisitos de segurança de um produto, quase uma ferramenta de padronização e avaliação da criptografia. Foram formuladas para oferecer uma avaliação imparcial de produtos de segurança, realizada por entidades neutras e por avaliadores independentes. Os produtos submetidos à análise são encaminhados voluntariamente pelos próprios fornecedores, e suas funcionalidades, tanto em conjunto quanto isoladamente, são examinadas minuciosamente. Durante a avaliação, os recursos de cada produto são testados conforme um conjunto preestabelecido de critérios específicos para cada categoria.

1.4.2 - Criptografia em trânsito e em repouso

Para tanto, a análise principal de que modelo de ferramenta será necessária se dá através

de entender se a soluções de criptografia de informações costumam ser organizadas com base na finalidade de proteção, entendendo se esta informação está destinada a dados armazenados ou àqueles em movimento.

Destarte dados em trânsito são considerados aqueles dados que se deslocam entre dispositivos, como em redes privadas ou pela Internet. Durante esse percurso, eles ficam mais vulneráveis, pois precisam ser cifrados antes da transferência e estão sujeitos às falhas inerentes aos métodos de transmissão. A encriptação efetuada durante o envio, conhecida como criptografia ponta a ponta, assegura que, mesmo se interceptados, os dados permaneçam confidenciais.

Já os dados em repouso são os dados que estão armazenados em dispositivos que não estão sendo utilizados ou transferidos ativamente.

Geralmente esses dados apresentam menor exposição a ataques, porque normalmente os mecanismos de segurança dos dispositivos restringem o acesso, embora não eliminem totalmente o risco, sua vulnerabilidade é exponencialmente menor. Ademais, por costumarem conter informações de maior valor, são alvos mais atrativos para agentes mal-intencionados.

A proteção dos dados armazenados reduz as chances de roubo decorrente de situações como o extravio ou furto de dispositivos, compartilhamento de senhas ou concessão acidental de permissões. Esse método também retarda o acesso indevido, proporcionando um tempo crucial para que o proprietário identifique a ocorrência de perda de dados, ataques de *ransomware* (agente que sequestra dados digitais), exclusão remota de informações ou alteração de credenciais.

Uma estratégia para proteger os dados em repouso é a utilização de T.D.E (*Transparent Data Encryption..*), que é uma tecnologia empregada para assegurar a proteção dos dados armazenados quando encriptando os bancos de dados diretamente no disco rígido e em suas mídias de backup. Contudo, ela não oferece cobertura para dados em transmissão sendo até hoje muito utilizada por empresas como a Microsoft, Oracle e IBM para cifrar arquivos de banco de dados.

1.5 Princípio da publicidade

Para além do descrito supra, dentro da esfera jurídica o princípio da publicidade é um dos pilares norteadores, pois garante a transparência dos atos e decisões processuais, permitindo a transparência das ações do Poder Judiciário e da administração pública. Fortalecendo assim a confiança dos cidadãos no sistema legal, possibilitando que as decisões sejam conhecidas.

> O princípio da publicidade, inserido no rol de princípios da Administração Pública, previstos no caput do art. 37 da Carta Magna de 1988, impõe a divulgação e a exteriorização dos atos do Poder Público. Tal imposição de transparência dos atos administrativos tem relação direta com o princípio democrático constitucional, possibilitando o exercício do controle social sobre os atos públicos. (SANTOS, Daniel; COSTA, Pâmela, 2022, p.61).

Desta feita, contribuindo para a construção de uma jurisprudência consistente e coerente, possibilitando que as razões de decidir sejam divulgadas e debatidas, dentro dos processos e sentenças disponíveis, sendo passível de verificar a uniformidade das decisões de diferentes turmas visando a melhoria do funcionamento público.

Entretanto, a aplicação do princípio da publicidade deve ser equilibrada com a necessidade de proteger direitos essenciais, como a intimidade dos envolvidos e a segurança dos procedimentos em determinadas fases processuais dependendo das informações e das partes envolvidas.

> Salienta-se que na hipótese de informações classificadas como sigilosas, consideradas imprescindíveis à segurança da sociedade ou do Estado, o sigilo é temporário e o respectivo prazo depende da classificação conferida à informação (SANTOS, Daniel; COSTA, Pâmela, 2022, p.62).

Esse equilíbrio é alcançado por meio de regras específicas que delimitam as situações em que o sigilo é imprescindível, garantindo que a transparência não comprometa a eficácia dos processos ou a proteção das partes, mantendo assim a legitimidade e a eficiência do sistema jurisdicional.

1.6 Funcionamento no judiciário

Com a implementação dos sistemas de processos eletrônicos, o princípio da publicidade, que por sua vez é subjetivo, ganha uma nova aplicação, que por sua vez passa a ter um contorno objetivo, pois ganha uma nova dimensão ao permitir o acesso em tempo real dos atos processuais.

Podendo ser posto como exemplo a justiça federal, através do Sistema de Processo Judicial Eletrônico (P.J.e), os documentos, despachos, sentenças e demais movimentações são registrados e disponibilizados em plataformas acessíveis via internet, ampliando assim a transparência de cada etapa do processo e o acesso ao mesmo.

Além disso, esses sistemas contam com interfaces intuitivas e ferramentas avançadas de busca, que possibilitam a localização rápida de informações pertinentes e a visualização de históricos detalhados do andamento contido nos autos. A integração entre diversos órgãos do Poder Judiciário, por meio de bases de dados e do Diário da Justiça Eletrônico, reforça o acesso uniforme e contribui para a padronização e a consistência dos registros processuais, tendo as audiências, como exemplo de publicidade.

Por fim, o ambiente digital dos processos judiciais demanda a implementação de medidas de segurança, como ferramentas de autenticação, criptografia e controle de acesso, assegurando que mesmo com a ampla publicidade dos atos, informações que podem comprometer a integridade e a intimidade dos envolvidos sejam tratadas com o devido sigilo quando necessário, visando desta forma equilibrar transparência e proteção dos direitos individuais.

Contudo, a aplicação da publicidade não é absoluta; ela deve ser nivelada com a proteção de direitos fundamentais, como a intimidade, a vida privada e a segurança das partes envolvidas.

> Entretanto, as informações pessoais, relativas à intimidade, à vida privada, à honra e à imagem, terão seu acesso restrito, independentemente de classificação de sigilo, com prazo máximo de 100 anos a contar da sua data de produção, aos agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e poderão ter autorizada sua divulgação ou acesso por terceiros diante da previsão legal ou consentimento expresso da pessoa a que elas se referirem. (SANTOS, Daniel; Costa, Pâmela, 2022, p.62).

Em situações específicas como em processos que envolvem menores ou temas sensíveis a divulgação de certos dados pode ser parcialmente restringida para preservar esses direitos, respeitando assim a dignidade da pessoa humana e a segurança dos envolvidos.

Conflito

2.1 Como as informações são tratadas no judiciário

A base para a proteção de dados está objetivamente alicerçada em dois pilares, a Lei Geral de Proteção de Dados (L.G.P.D.) e a Lei de Acesso à Informação (L.A.I).

A L.G.P.D (Lei nº 13.709/2018) regula dentro de outras coisas, a responsabilidade pela coleta, pelo armazenamento, pelo tratamento e o compartilhamento de dados pessoais bem como de informações sensíveis, criada para proteger a privacidade e os direitos fundamentais dos cidadãos, exigindo que empresas e órgãos públicos sejam transparentes quanto ao uso das informações, sendo que em caso de descumprimento a L.G.P.D prevê sanções que podem variar de advertências a multas.

Já a Lei de Acesso à Informação (Lei nº 12.527/2011) é a legislação brasileira que estabelece o acesso às informações públicas preservando o princípio da publicidade determina que órgãos e entidades dos poderes Executivo, Legislativo e Judiciário, bem como do Ministério Público, devem disponibilizar, de forma proativa ou mediante solicitação, dados e documentos de interesse coletivo, ressalvadas as exceções legais que protegem a segurança do Estado, a vida privada e outros interesses relevantes.

Destarte, a L.A.I já estabelece as diretivas para que documentos com conteúdo sensível sejam tratados com rigor de quem os acessa e para o seu armazenamento:

> Pela LAI: a) ultrassecreta: 25 anos de sigilo, prorrogável uma única vez; b) secreta: 15 anos de sigilo; e c) reservada: cinco anos de sigilo. Ao final do prazo de classificação, ou consumado o evento que defina o seu termo final,

> a informação tornar-se-á, automaticamente, de acesso público, nos termos da LAI. (SANTOS, Daniel, 2022, p.62).

Para além desses documentos, quando envolvem partes sensíveis como menores de idade ou temas específicos as informações das partes envolvidas são anonimizadas para que não ocorra identificação.

Todavia essa metodologia não ocorre de forma automática, mas sim a requerimento, direcionado ao magistrado, não sendo muitas vezes deferidas, podendo causar problemas sérios quanto a vazamento de informações e danos aos envolvidos causando assim violação direta a preceitos constitucionais.

Por essa feita, recai sobre os ombros do STF a uniformização desse controle por parte do judiciário quanto ao acesso sem a violação do princípio da publicidade, assim evitando um conflito claro de preceitos fundamentais, sem furto de competência das esferas estaduais ou mesmo federais.

2.2 Como esses dados podem ser utilizados de maneira indevida

Como mencionado supra, o deferimento ou tratamento de dados sensíveis dentro do judiciário nem sempre seguem diretrizes claras, assim como o acesso a essas informações para o público que tem interesse em decisões, mas não conseguem acesso mostra como esse assunto é sensível e estratégico.

Assim, os dados disponíveis que incluem informações sobre processos, partes envolvidas e decisões, podem ser explorados maliciosamente de diversas maneiras.

Podendo ser utilizado para construção de perfis detalhados, juntando informações de diferentes processos pode permitir a criação de perfis completos de indivíduos ou empresas, pois estão disponíveis dados como nomes, endereços, históricos de litígios e relacionamentos processuais, assim quando são combinados podem identificar vulnerabilidades pessoais ou institucionais. Podendo ser usados para golpes de engenharia social, onde o agente se passa por alguém de confiança para obter mais informações ou ter acesso a recursos financeiros.

Para além disso, é utilizado para a falsificação e manipulação de documentos. Da mesma maneira que mencionado supra as informações detalhadas podem levar ao risco de criação de documentos falsos ou a alteração de registros.

Utilizados também para prejuízo à reputação e extorsão, assim, as mesmas informações podem ser utilizadas para chantagem, afetando a reputação e causando danos profissionais e pessoais.

Podem também ser aplicadas nos casos de campanhas de desinformação, sendo a informação manipulada e divulgada seletivamente para criar narrativas enganosas, influenciar a opinião pública e gerar confusão, minando a legitimidade das instituições.

Segundo dados de relatórios da I.B.M (2024), grande empresa do segmento de tecnologia, o custo de um vazamento de dados pode girar em torno de 4,8 milhões de dólares.

> O custo médio global de uma violação de dados aumentou 10% em um ano, chegando a US$ 4,88 milhões, o maior salto desde a pandemia. A interrupção dos negócios e as atividades de resposta pós-violação foram responsáveis pela maior parte desse aumento anual de custos (IBM, 2024, p.8).

Outrossim, para além dos motivos sociais, a utilização de dados sensíveis contidos no sistema judiciário pode causar custos para a sociedade por volta de milhões de reais, para tanto, o relatório demonstra um aumento na violação de dados pessoais identificado:

> Quase metade de todas as violações envolveram informações pessoais identificáveis (PII) de clientes, que podem incluir números de identificação fiscal, e-mails, números de telefone e endereços residenciais. Registros de propriedade intelectual (PI) ficaram em segundo lugar (43% das violações). O custo dos registros de PI aumentou consideravelmente em relação ao ano passado, para US$173 por registro no estudo deste ano, em comparação com US$156 por registro no relatório do ano passado. (IBM, 2024, p.4).

Em suma, esse relatório com dados gigantescos demonstra que a proliferação e captura de dados sensíveis, como é o exemplo do poder judiciário, está aumentando os riscos de violação, vejamos:

> 35% das violações envolveram dados ocultos, mostrando que a proliferação de dados está dificultando o rastreamento e a proteção. O roubo de dados ocultos está correlacionado a um custo 16% maior de uma violação. Os pesquisadores descobriram que armazenar dados em diferentes ambientes provou ser uma estratégia de armazenamento comum, responsável por 40% das violações. Essas violações também levaram mais tempo para serem identificadas e contidas. Por outro lado, os dados armazenados em apenas um tipo de ambiente foram violados com menos frequência, que esse ambiente fosse de nuvem pública (25%), no local (20%) ou nuvem privada (15%). (IBM, 2024, p.4).

Assim, a implementação de diretrizes únicas para manutenção da segurança e preservação de princípios constitucionais, se mostra uma necessidade, sendo o STF responsável pelos motivos supra por essa uniformização de dados e protocolos no sistema judiciário.

2.3 Como as decisões do STF se encaminham na sua proteção

Isto posto, a principal decisão que define as diretrizes da relação entre a publicidade necessária e a proteção de dados pelo poder judiciário/público, está contida na ADI 6.649/DF de 15.09.2022, com relatoria do Ministro Gilmar Mendes, que já relaciona que as medidas públicas

devem se basear pelo princípio da publicidade, todavia reconhece a problemática da questão.

> Se é certo que informações gerais relacionadas à atividade administrativa devem, em regra, se submeter ao princípio da ampla publicidade, não é menos exato que o tratamento de dados pessoais segue lógica diversa, focada na salvaguarda da privacidade dos cidadãos. Essa distinção impõe regime jurídico híbrido para o tratamento das informações coletadas ou produzidas pela Administração Pública, a depender do maior ou menor vínculo que elas guardem com atributos da personalidade ou qualidades próprias do cidadão. (BRASIL, STF, 2022, p. 45)

Nela o pleno da casa reconhece o conflito disposto, entendendo a necessidade de tornar público os atos, todavia reconhecendo os perigos do acesso irrestrito:

> O tratamento de dados pessoais promovido por órgãos públicos que viole parâmetros legais e constitucionais, inclusive o dever de publicidade fora das hipóteses constitucionais de sigilo, importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa. (BRASIL, STF, 2022, p.4)

Desta forma, compreender que o estado será responsabilizado, bem como os seus agentes, é de medida fundamental para alicerçar seus parâmetros. Para além disso, ainda demonstra que a pessoa que disponibilizar seus dados deve ter acesso às informações distribuídas, assim como em que sentido foram usadas pelo poder público, sendo que este está delimitado pela legitimidade de suas funções.

> Em segundo, estabeleceu-se que a incidência do princípio da transparência impõe que a Administração Pública garanta ao titular dos dados um nível de controle suficiente para a verificação prospectiva da licitude do tratamento de dados. Isso se desdobraria, de acordo com a decisão, em um dever de publicidade que seja capaz de fornecer ao cidadão condições mínimas de proceder a um controle da forma como o Estado lida com dados pessoais. (BRASIL, STF, 2022, p. 27)

Entendendo essa delimitação de tratamento, a decisão ainda estabelece que deve seguir as diretrizes, quando possível, da LGPD, tendo em vista que referida norma foi legislada para delimitar as relações privadas do tratamento de dados e não especificamente do direito público.

Estabelece assim diretrizes para que as informações sejam utilizadas:

> O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco 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. (BRASIL, STF, 2022, p. 69).

Assim, a criptografia de dados se estabelece como ferramenta a ser utilizada para alcançar o objetivo maior de proteção, utilizado de forma a concretizar o estabelecido em lei e ratificado pelo STF.

Possíveis soluções

3.1 Análise: como as decisões do STF podem encaminhar o judiciário para uma maior proteção

Como descrito, as diretrizes sobre a utilização dos dados pessoais do pelo poder judiciário/público nas decisões do STF, estão direcionadas a uma maior proteção dos dados, restringindo assim quando necessário seu acesso, flexibilizando esse princípio.

É inegável a possibilidade de utilização de forma irregular desses dados, principalmente com a facilidade de acesso através de meios digitais. Desta maneira, não há como vislumbrar qualquer decisão que não seja direcionada nesse sentido.

Ao analisar o tema proposto, é possível visualizar a criptografia servindo de auxiliar para esse desafio, quando empregados de forma estratégica e direcionada podem ser a solução para esse controle, todavia o desafio é gigantesco.

O principal problema para isso é a divisão de sistemas dentro do poder judiciário, principalmente quando tratamos da esfera estadual, visto que a federal ainda conta com uma unidade de sistema, o PJ-e.

Todavia, ao verificar as esferas estaduais, temos diferentes estados com sistemas distintos, fazendo com que a falta de unidade faça com que vulnerabilidades ocorram, sendo visto que só nos sistemas mais utilizados já temos uma grande fragmentação, como o caso do E-proc, E-SAJ, entre outros.

Outrossim, ao direcionar como esses dados devem ser tratados, o STF, pode ter colocado diretrizes que visam uma unificação sistêmica para esse segmento, colocando bases que podem ser utilizadas para justificar a utilização da ferramenta criptografia como forma de solucionar o desafio.

3.2 Como a criptografia é utilizada em diferentes países para solução desse problema

Outros países já enfrentaram problemas parecidos, tendo soluções estratégicas úteis que podem servir de lição para implementação no nosso judiciário.

Como é o caso dos países europeus que sofrem constantemente com a tentativa de invasão de dados, como visto no estudo da Prof. Me. Ana Rita Vaz, o seu estudo para a universidade de Coimbra:

> Um estudo da Gemalto relativo à primeira metade de 2017, revela números assustadores relativos a incidentes de violação de dados pessoais. É, aí, revelado que uma média de 10,507,550 de registros de dados foram perdidos ou roubados diariamente. Isto significa um aumento significativo de 164% em dados roubados, perdidos ou comprometidos, relativamente à segunda metade de 2016. Sublinha-se também o facto de menos de 5% destas violações terem sido "*safe breaches*" que consistem naquelas em que a encriptação torna inúteis os dados roubados. (Vaz, Ana Rita Francisco., 2018, p.9)

Para tanto, o uso de criptografia é aplicado de maneira corrente na Europa, ou mesmo os acessos são restritivos quando necessários, não sendo tolerado a passagem de dados físicos sem proteção, fato esse comum em determinados setores do judiciário, como observado nessa passagem de estudo sobre a *GDPR - GENERAL DATA PROTECTION REGULATION*, lei ao qual nossa LGPD foi baseada:

> É aconselhável demonstrar que a empresa trata de maneira adequada a privacidade dos dados pessoais, na medida em que arquivos ou transmissões de dados pessoais utilizam técnicas de criptografia ou similar para aumentar a segurança do sigilo e acesso aos dados pessoais. Armazenar em um *pen driver* dados pessoais de clientes e funcionários sem criptografia demonstra uma falta de proteção adequada. (FONTES, Edison, 2018, p.4)

Muitas dessas práticas já são utilizadas no Brasil por meio da LGPD, mas como mencionado supra, essas práticas foram destinadas para as relações privadas, e não necessariamente para o poder judiciário e suas especificidades.

3.3 Possíveis formas de equilíbrio de criptografia de segurança com a publicidade disposto na decisão do STF

Em primeira análise, uma solução para esse conflito é a unificação de sistemas, tanto pelos tribunais estaduais como pela justiça federal, porém entra em conflito com a autonomia de poderes dificultando sua aplicação prática. Destarte, podemos pensar em um protocolo utilizado de forma unitária apenas para a manutenção da informação, tanto aquela em trânsito, quanto aos dados em repouso.

Para o trânsito uma criptografia robusta, onde se possa identificar a quem está sendo direcionado os dados utilizados ou mesmo barrando informações que possam ser interceptadas, podendo ser utilizado criptografia de ponta a ponta para garantir a integridade da informação. Sendo necessário para acesso chaves únicas, já utilizadas no sistema pelos advogados, porém não para o público em geral.

Nessa feita, esse acesso público que por advogados já é realizado por intermédio de certificado digital, poderá ser feito para o público em geral através do sistema do governo federal GOV.BR, que já agrupa uma série de informações em um banco de dados controlado e seguro, podendo assim as informações serem rastreadas até quem teve acesso efetivo a ela, sendo uma parceria entre o judiciário e o poder executivo.

Diminuindo em sua medida fragilidades no sistema, visto que estando em plataforma robusta e já utilizada para validação de quem acessa as informações sensíveis.

Para além disso, a criptografia pode ser empregada para os dados em repouso, como em processos arquivados, visto que sua utilização já não é ativa, porém sua preservação é matéria de direito. Para esses dados, se vislumbra uma central unitária de banco de dados, uma parceria entre os tribunais, para diminuir fragilidades e acessos de forma irrestrita, sendo esse codificado em TDE, com local unitário e limitação de acesso através de criação de plataforma própria, aumentando assim a proteção, porém garantindo o acesso de todos.

Desta feita, quando olhamos as possíveis soluções, conseguimos vislumbrar uma mudança possível da unificação do judiciário, visando maior celeridade e união entre as esferas da prestação jurisdicional.

Conclusão

Em conclusão, as decisões do STF, exemplificadas pela ADI 6.649/DF de 15.09.2022, mostram o desafio de harmonizar o princípio da publicidade com a proteção dos dados pessoais na atuação do poder judiciário. O entendimento firmado evidencia que, embora seja imprescindível que os atos da Administração sejam transparentes e acessíveis à sociedade, os dados pessoais exigem um tratamento diferenciado resguardando a informação sensível.

Assim, a criptografia como ferramenta de segurança, é uma resposta estratégica para esse desafio, sendo aplicada de forma robusta contribuindo para minimizar os riscos de acesso indevido e vazamentos, sem renunciar à publicidade que é essencial para o controle social dos atos públicos, vislumbrando uma possível cooperação dos sistemas existentes, podendo os diferentes poderes criar um sistema único seguro e controlado.

Portanto, os alicerces dispostos pelo STF apontam para um caminho que, embora desafiante, é fundamental para promover um equilíbrio sustentável entre a ampla divulgação dos atos públicos e a proteção dos dados individuais.

Referências

1. BOFF, Salete Oro; VESOLOSKI, Simone Paula; MORAIS, José Luis Bolzan de; SCHNEIDER, Leonardo Calice (Orgs.). *Impactos jurídico-políticos da tecnologia.* Porto Alegre: Editora Fi, v. 1, 2022.

2. BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade 6.649 Distrito Federal.* Brasília: STF, 15 set. 2022.
3. FONTES, Edison. *GDPR - General Data Protection Regulation - Considerações Iniciais.* Porto Alegre: Direito & TI, 2018.
4. IBM. *Relatório do custo das violações de dados 2024.* IBM Security, 2024.
5. MACHADO, Diego; DONEDA, Danilo. *Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados.* São Paulo: Revista dos Tribunais, v. 998, Caderno Especial, p. 99-128, dez. 2018.
6. RICHTER, Alexandre Lima. *Acesso à informação na segurança pública: o uso de criptografia no banco de dados.* Recima21 – Revista Multidisciplinar, v. 6, n° 2, 2025.
7. SANTOS, Daniel Gasparotto dos; COSTA, Pâmela Taís da. *Impactos jurídico-políticos da tecnologia - Volume 1, O Papel da Tecnologia na Tentativa de Efetivar a Transparência na Licitação por Adesão.* Porto Alegre: Editora Fi, 2022.
8. TERADA, Roudo. *Segurança de dados: criptografia em redes de computadores.* São Paulo: Editora Blucher, 2011.
9. VAZ, Ana Rita Francisco. *O Regulamento Geral de Proteção de Dados: Desafios e Impactos.* 2018. Dissertação (Mestrado) – Universidade de Coimbra, Coimbra, Portugal.