NOTÍCIAS E DECISÕES SOBRE DIREITO DIGITAL, LGPD E PROTEÇÃO DE DADOS

Incidentes de Segurança com Dados Pessoais: comunicar é preciso, mas nem sempre!

A matéria destaca que os incidentes de segurança com dados pessoais continuam sendo recorrentes e muitas vezes graves, como no caso recente do vazamento de 16 bilhões de senhas em bancos de dados diferentes.

A **LGPD (Lei 13.709/2018)** impõe aos controladores e operadores a obrigação de proteger os dados pessoais contra acessos não autorizados, falhas ou situações ilícitas.

Pelo **artigo 48 da lei**, é necessário comunicar à ANPD e aos titulares sempre que um incidente possa gerar risco ou dano relevante, o que foi regulamentado pela **Resolução CD/ANPD nº 15/2024 (RCIS)**, que define prazos, formatos e requisitos da comunicação.

Um incidente de segurança é qualquer evento confirmado que afete a confidencialidade, a integridade, a disponibilidade ou a autenticidade dos dados pessoais, seja por ação maliciosa ou acidental. No entanto, nem todo incidente precisa ser comunicado, já que cabe ao controlador avaliar se há efetivamente risco ou dano relevante ao titular.

Para essa avaliação, a RCIS prevê a análise de fatores como a presença de dados sensíveis, dados de crianças, informações financeiras, o volume em larga escala ou outros impactos possíveis à vida dos titulares.

O **Serpro**, por exemplo, já possuía antes da LGPD um **Plano de Resposta a Incidentes de Segurança com Dados Pessoais (PRIDP)**, que envolve equipes internas e o encarregado de proteção de dados. Esse plano adota uma matriz de risco que cruza impacto e probabilidade. O impacto é avaliado considerando o tipo de dado, a possibilidade de identificar o titular, a relevância, eventuais interrupções de serviços e até mesmo a intenção maliciosa. Já a probabilidade refere-se à chance de o incidente realmente afetar direitos fundamentais dos titulares.

Com base no resultado dessa análise, são definidas as medidas a serem adotadas:

Incidentes de **risco baixo** devem ser apenas registrados e controlados para fins de prestação de contas;

os de **risco médio** podem levar à divulgação pública no site, acompanhada de recomendações aos titulares;

já os de **risco alto** exigem comunicação direta aos titulares ou nota pública, além da notificação à ANPD.

Não basta a ocorrência de um incidente para que a comunicação seja obrigatória. É essencial avaliar de forma criteriosa se o evento gera risco ou dano relevante, agindo com rapidez e método. Ter um plano estruturado e transparente garante não só a conformidade com a LGPD, mas também a proteção efetiva dos titulares e da própria organização.

Link: https://repositorio.usp.br/directbitstream/8bb39ff3-ee70-4117-8d5d-101830518acb/HSP_14_2025.pdf

Governo abre consulta pública sobre a criação da Política de Governança e Compartilhamento de Dados

O governo federal iniciou, em **23 de julho de 2025**, uma consulta pública para discutir com a sociedade a criação da Política de Governança e Compartilhamento de Dados, disponível para contribuições até **7 de agosto** ou **22 de agosto**, conforme diferentes fontes.

A proposta busca assegurar que os dados sejam utilizados de forma estratégica no aprimoramento de políticas públicas e serviços públicos, com base na infraestrutura nacional de dados conhecida como "Base de Dados do Brasil" ou Infraestrutura Nacional de Dados (IND), que congrega normas, políticas, ferramentas e pessoas para integrar, qualificar, abrir e proteger dados.

O texto da minuta do decreto foi elaborado pelo Comitê Central de Governança de Dados (CCGD), que envolveu participações da sociedade civil, e está disponível na plataforma Brasil Participativo para receber sugestões da população.

Entre as inovações da proposta está a criação da figura do Executivo de Dados, equivalente ao cargo de Chief Data Officer (CDO), que atuará no nível estratégico de cada órgão ou entidade federal, de forma independente da área de tecnologia da informação, com prazo de 60 dias para indicação desse responsável.

Além disso, cada instituição deverá identificar servidores encarregados da gestão de dados (curadores), que trabalharão alinhados aos Executivos de Dados, aos Gestores de TI e aos Encarregados de Dados Pessoais, atuando na curadoria, catalogação, qualidade, disponibilidade e proteção das bases de dados.

RAYES e FAGUNDES

A proposta também estabelece diretrizes para interoperabilidade e compartilhamento de dados entre sistemas governamentais federais, alinhadas à LGPD, com o objetivo de melhorar a execução de políticas públicas e evitar que cidadãos precisem fornecer repetidamente suas informações, além de facilitar a demanda de dados entre entes federativos.

A minuta prevê a adoção de registros de referência, fontes padronizadas e reutilizáveis (como nome, data de nascimento, CEP, municípios etc.) a serem formalizados pelo CCGD e utilizados obrigatoriamente por todos os órgãos federais, de modo a garantir consistência e eficiência na prestação de serviços públicos.

Outro ponto sensível do texto também estabelece regras sobre o tratamento de dados em ambientes externos: dados com grau de sigilo legal ou regulamentar não poderão ser hospedados fora da administração pública e devem seguir normas de segurança definidas pelo Gabinete de Segurança Institucional, sendo recomendada a utilização da Nuvem de Governo para esse tipo de dado.

Essa iniciativa integra a agenda digital do governo, que contempla ações como o fortalecimento da Base de Dados do Brasil: uma infraestrutura que permite integrar diferentes bases (como educação, saúde, assistência social, uso de equipamentos públicos, propriedade rural etc.) para personalizar serviços, automatizar benefícios, integrar níveis de governo e melhorar gestão e combate a fraudes, conforme destacaram representantes como a ministra Esther Dweck. A proposta reflete, assim, um avanço na cultura de governança de dados na administração pública federal, onde dados se tornam ativos estratégicos, tratados dentro de uma lógica orientada por qualidade, segurança, reuso, transparência e eficiência na formulação e execução de políticas públicas.

Link: https://repositorio.usp.br/directbitstream/8bb39ff3-ee70-4117-8d5d-101830518acb/HSP_14_2025.pdf

Brasil posiciona-se na vanguarda global da gestão de dados em saúde

No dia 23 de julho de 2025, foi publicado o **Decreto nº 12.560/2025**, que institui a Rede Nacional de Dados em Saúde (RNDS) e as Plataformas SUS Digital, consolidando a política do Ministério da Saúde para a transformação digital do Sistema Único de Saúde (SUS). Esse decreto representa um avanço estratégico para o país, posicionando-o na vanguarda global da gestão de dados em saúde e abrindo novas portas para a inovação e a resolução eficiente do cuidado.

O texto normativo estabelece diretrizes claras para o uso compartilhado e o tratamento de dados pessoais de saúde, sempre em conformidade com a LGPD. O compartilhamento deve ser proporcional ao fim público do SUS, e torna obrigatória a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais, que detalha os riscos e as medidas mitigadoras. Também proíbe o uso secundário desses dados para finalidades incompatíveis, como campanhas publicitárias sem consentimento.

A RNDS é formalizada como plataforma nacional interoperável que integra dados do SUS, como dados, clínicos, administrativos, financeiros e cadastrais, em todo território nacional.

O decreto limita o uso dos dados a finalidades relativas a atendimento, vigilância, gestão, pesquisa e políticas públicas, garantindo soberania tecnológica, segurança, privacidade, integridade e continuidade do cuidado. A alimentação da rede será feita por meio de estabelecimentos públicos e privados, dentro de modelos padronizados, assegurando integração, consistência e uso seguro das informações.

RAYES e FAGUNDES

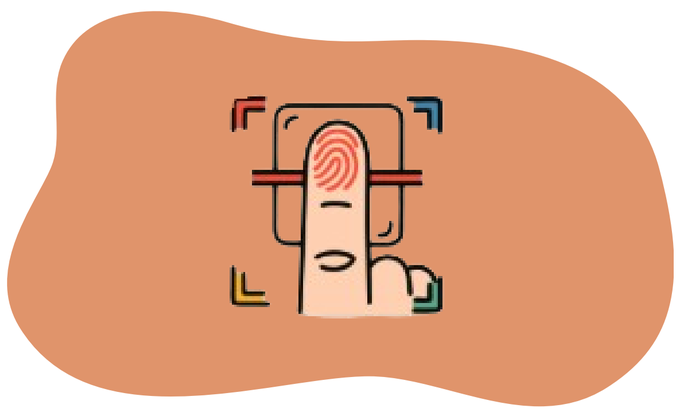
O compartilhamento de dados ocorrerá segundo normas da LGPD e será restrito a entidades públicas, gestores de saúde e órgãos de pesquisa, sempre com base em princípios de interoperabilidade, segurança, privacidade, centralidade no cidadão, padronização, transparência, uso ético e eficiência. A governança da RNDS ficará a cargo do Ministério da Saúde, que regulamentará responsabilidades, transparência e gestão dos agentes envolvidos.

As Plataformas SUS Digital, por sua vez, foram concebidas como canais que simplificam o acesso a informações e serviços de saúde para usuários do SUS, profissionais e gestores, promovendo transformação digital, equidade, inclusão e inovação. Essas plataformas visam ampliar o acesso aos dados, fortalecer a continuidade do cuidado e oferecer suporte estratégico à gestão pública, com vistas ao aprimoramento dos serviços de saúde.

O decreto reforça o ecossistema de saúde digital do SUS, posicionando o Brasil como referência mundial na gestão de dados em saúde, estimulando a proteção de dados e a segurança da informação, reduzindo desigualdades regionais no acesso aos serviços digitais, e gerando inovação científica e tecnológica, especialmente com o uso de inteligência artificial. Além disso, ele permite uma leitura mais precisa das necessidades de saúde da população brasileira, melhor planejamento e políticas públicas mais eficazes, além de fomentar uma governança cooperativa no modelo federalista do SUS.

Link: https://repositorio.usp.br/directbitstream/8bb39ff3-ee70-4117-8d5d-101830518acb/HSP_14_2025.pdf

Biometria no Estado Digital: Proteção de dados como eixo estratégico



O artigo, publicado no portal Migalhas, analisa os **Decretos Federais nº 12.561 e nº 12.564**, ambos de julho de 2025, que estabelecem a verificação biométrica obrigatória para a concessão de benefícios previdenciários e a formalização digital do crédito consignado, respectivamente.

Esses decretos posicionam a biometria como um elemento central na transformação digital do Estado, integrando inovação tecnológica com a proteção de dados pessoais sensíveis, conforme previsto na Lei Geral de Proteção de Dados (LGPD).

O **Decreto nº 12.561/25** institui a verificação biométrica obrigatória para a concessão de benefícios previdenciários, priorizando a Carteira de Identidade Nacional (CIN) como base primária de identificação

Para garantir a inclusão digital e evitar exclusões, o decreto permite o uso de bases transitórias, como a Carteira Nacional de Habilitação (CNH), registros da Polícia Federal e do Tribunal Superior Eleitoral (TSE), até que a CIN seja universalizada. Essa abordagem visa assegurar a continuidade do acesso aos benefícios enquanto se implementa a nova infraestrutura de identificação digital.

O **Decreto nº 12.564/25** regula a formalização digital do crédito consignado, exigindo prova de vida biométrica e consentimento explícito do trabalhador. Esse consentimento deve ser registrado de forma eletrônica, auditável e vinculada à operação, garantindo que o titular mantenha controle efetivo sobre seus dados. Além disso, o decreto estabelece a necessidade de evidências técnicas, como vídeos em tempo real com movimentos específicos, para comprovação de vida, alinhando-se às melhores práticas de segurança e confiabilidade.

A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central na supervisão desses processos, conforme os artigos 4º, §3º, 38 e 55-J, XIII da LGPD. A ANPD pode solicitar relatórios de impacto à proteção de dados, emitir recomendações técnicas e intervir em casos de uso indevido ou vazamento, fortalecendo a governança e a segurança jurídica desses sistemas.

Embora a implementação da biometria digital ofereça benefícios significativos, como a prevenção de fraudes e a ampliação da confiança pública, também apresenta desafios, especialmente em relação à inclusão digital. Idosos, pessoas em áreas rurais e cidadãos com limitações de acesso digital podem ser afetados por um modelo excludente

Para mitigar esses riscos, os decretos incorporam mecanismos inclusivos, permitindo o uso de bases alternativas e processos híbridos até que a CIN seja universalizada.

Em conclusão, **os decretos nº 12.561 e nº 12.564/25** representam um marco na modernização dos serviços públicos e financeiros no Brasil, equilibrando inovação tecnológica com a proteção de dados pessoais sensíveis. Ao integrar a biometria como ferramenta central, o Estado Digital brasileiro avança na construção de um sistema mais eficiente, seguro e inclusivo, alinhado às melhores práticas internacionais de proteção de dados.

Link: https://www.migalhas.com.br/depeso/435886/biometria-no-estado-digital-protecao-de-dados-como-eixo-estrategico

Governo prepara lista com nomes de impedidos de apostar

O governo brasileiro está desenvolvendo uma plataforma para identificar e bloquear usuários impedidos de realizar apostas online. A ferramenta, coordenada pelo Ministério da Fazenda, visa fornecer às casas de apostas uma lista de pessoas que devem ser excluídas, incluindo :

- beneficiários do Bolsa Família
- menores de 18 anos
- atletas profissionais
- árbitros
- técnicos esportivos
- pessoas diagnosticadas com ludopatia (vício em jogos)
- autoexcluídos
- aqueles proibidos judicialmente

As empresas de apostas terão a obrigação de recusar cadastros, depósitos ou apostas desses indivíduos. Caso algum nome da lista já esteja registrado em uma plataforma, deverá ser bloqueado e ter os valores devolvidos. No entanto, representantes do setor solicitam uma plataforma unificada para facilitar a implementação dessas restrições.

Vale destacar que, a criação dessa lista reflete a preocupação do governo com jogos responsáveis e prevenção de fraudes, atuando de forma preventiva para proteger grupos vulneráveis e evitar problemas sociais ligados ao vício em apostas. Também é importante notar que a medida exige integração tecnológica eficiente entre órgãos públicos e plataformas privadas, o que pode gerar desafios operacionais e regulatórios. Por fim, a iniciativa sinaliza maior fiscalização do setor de apostas online, indicando que o governo busca equilibrar o crescimento da indústria com proteção legal e social aos cidadãos.

Link: https://www.migalhas.com.br/depeso/435886/biometria-no-estado-digital-protecao-de-dados-como-eixo-estrategico

Decisões

STJ - REsp 2.139.749

RECURSO ESPECIAL. MARCO CIVIL DA INTERNET. PROVEDOR DE APLICAÇÃO. PLATAFORMA DE VÍDEO. PANDEMIA DA COVID-19. TERMOS DE USO. DESINFORMAÇÃO. MODERAÇÃO DE CONTEÚDO. REMOÇÃO. LEGITIMIDADE. NOTIFICAÇÃO PRÉVIA. SHADOWBANNING. NÃO OCORRÊNCIA. LIBERDADE DE EXPRESSÃO. CONDICIONANTES.

1. A controvérsia jurídica consiste em definir se (i) o provedor de aplicação de internet (no caso, plataforma de vídeo) pode remover conteúdo de usuário que violar os termos de uso e se (ii) tal moderação de conteúdo encontra amparo no ordenamento jurídico.

2. Ausente o prequestionamento, e não tendo sido opostos embargos de declaração para suprir a deficiência, aplicam-se as Súmulas nºs 282 e 356/STF.

3. Não configura cerceamento de defesa o julgamento antecipado da lide ante a suficiência dos elementos documentais. Tema 437/STJ.

4.Os termos de uso dos provedores de aplicação, que autorizam a moderação de conteúdo, devem estar subordinados à Constituição, às leis e a toda regulamentação aplicável direta ou indiretamente ao ecossistema da internet, sob pena de responsabilização da plataforma.

5. Moderação de conteúdo refere-se à faculdade reconhecida de as plataformas digitais estabelecerem normas para o uso do espaço que disponibilizam a terceiros, que podem incluir a capacidade de remover, suspender ou tornar indisponíveis conteúdos ou contas de usuários que violem essas normas.

6. O art. 19 da Lei Federal nº 12.965/2014 ("Marco Civil da Internet") não impede nem proíbe que o próprio provedor retire de sua plataforma o conteúdo que violar a lei ou os seus termos de uso. Essa retirada pode ser reconhecida como uma atividade lícita de compliance interno da empresa, que estará sujeita à responsabilização por eventual retirada indevida que venha a causar prejuízo injustificado ao usuário.

7. Shadowbannig consiste na moderação de conteúdo por meio do bloqueio ou restrição de um usuário ou de seu conteúdo, de modo que o banimento seja de difícil detecção pelo usuário (assimetria informacional e hipossuficiência técnica). Pode ser realizado tanto por funcionários do aplicativo quanto por algoritmos e, em tese, caracterizar ato ilícito, arbitrariedade ou abuso de poder. Não ocorrência, no presente caso.

8. Recurso especial parcialmente conhecido e não provido.

(REsp n. 2.139.749/SP, relator Ministro Ricardo Villas Bas Cueva, Terceira Turma, julgado em 27/8/2024, DJe de 30/8/2024.)