A armadilha dos “dados não sensíveis”: o erro caro para as empresas

Data: 2025-10-01 13:19:23

Autor: Inteligência Against Invaders

Stefano Gazzella**:1 Outubro 2025 15:17**

Um argumento maravilhosamente difundido entre aqueles que trabalham com dados pessoais é o de subestimar os riscos ou se recusar a abordá-los. Essa é a crença de que não há necessidade de se preocupar com o processamento de dados “não confidenciais”. A premissa ontológica para a busca de soluções e medidas corretivas nas áreas de legalidade e segurança é a capacidade de fazer as perguntas certas. É por isso que uma tendência a ser excessivamente fácil *Ignorar dados* não pode constituir uma estratégia funcional ou mesmo minimamente útil.

É claro existem dados confidenciais sob o GDPR e requer altos níveis de proteção. No entanto, isso não significa que todos os outros tipos de dados (indevidamente chamados de *“comum”* por aqueles que simplesmente precisam criar categorias desnecessárias) podem ser dispensados em termos de gerenciamento de risco adequado. Não-sensível não pode de forma alguma significar “desprotegido”, nem mesmo através da interpretação mais inescrupulosa.

Falta de escrúpulos ou imprudência?

Enquanto a imprudência envolve comportamentos que selecionam opções econômicas em desafio às regras, forçando os titulares dos dados a pagar os custos de segurança, a fonte de comportamentos que levam a subestimar a importância de proteger *todo* Os dados pessoais são frequentemente atribuíveis a uma falta genuína de conhecimento. Cuidado: essa suposição não abre a porta para cenários menos graves ou aqueles em que um nível mais baixo de responsabilidade pode ser possível.

Hackear dados não confidenciais, como informações de identificação simples, pode ter consequências devastadoras para o titular dos dados. Considere que a maioria dos ataques de phishing envolve informações de contato, com maior probabilidade de sucesso se o acesso incluir informações como hábitos de consumo ou outras informações que podem ser expressas ou inferidas, mas não são particularmente confidenciais. A possibilidade de vincular informações a um titular de dados, de fato, os expõe a maiores riscos de roubo de identidade, fraude ou uma série de consequências desagradáveis que infelizmente fazem parte da vida digital cotidiana.

A disponibilidade desses dados para os cibercriminosos decorre das atividades do OSINT, mas também da capacidade de encontrar bancos de dados violados. Esses bancos de dados são violados como resultado de ações realizadas usando informações de contato simples e são enriquecidos por meio de novas violações, aumentando a eficácia das campanhas de ataque subsequentes.

Ignorar tudo isso é, hoje em dia, **injustificável** para uma organização que realiza atividades sobre dados pessoais, independentemente da maturidade dos dados.

Refletir sobre o uso sustentável de dados pessoais.

A questão da segurança e das violações de dados é, portanto, um argumento particularmente convincente para não subestimar a proteção de todos os dados pessoais, mas há um fator adicional: a legalidade do processamento. Embora a segurança do processamento seja um requisito do GDPR, também existem outras violações recorrentes que devem aumentar a conscientização sobre o impacto da violação das “regras do jogo” desde o início, como:

- não informar as partes interessadas de forma clara e completa (= violar o princípio da transparência);
- contornar as regras e não garantir direitos (= violar o princípio da equidade);
- coletar e processar dados sem seguir uma lógica (= violar o princípio da licitude, limitação de finalidade e minimização);
- Nunca exclua dados que não sejam mais úteis (= viole o princípio da limitação de armazenamento).

Obviamente, tudo isso leva à criação de bancos de dados fora do controle consciente do titular dos dados. E cria oportunidades fáceis de lucro para os cibercriminosos, uma vez que a falta de estratégia, como a evidente nas violações citadas acima, leva ao acúmulo de dados sem criar valor. E na ausência de valor, não há percepção de qualquer *ativo* precisando ser protegido.

A solução é pensar no uso sustentável dos dados pessoais. A lei especifica e regula as responsabilidades, mas uma abordagem estratégica correta sabe pensar em termos de valor gerado e não focar exclusivamente nos componentes de custo, como encontrar desculpas ou justificativas para fazer o *Mínimo* .

Caso contrário, é fácil cair em armadilhas, como a crença de que apenas dados confidenciais precisam ser protegidos ou monitorados. Isso cria todos os pontos cegos de gestão que inevitavelmente levam à inadequação das medidas em vigor.

Alerta de spoiler: Os titulares dos dados estão cientes disso. E é improvável que eles selecionem serviços daqueles que não podem garantir o uso sustentável de seus dados.

Stefano Gazzella
Diretor de Privacidade e Diretor de Proteção de Dados, atua como Consultor Jurídico da Área Jurídica. É especializada em proteção de dados pessoais e, na gestão da segurança da informação dentro das organizações, presta especial atenção às questões relacionadas com a engenharia social.
Chefe do comitê científico da Assoinfluencer, coordena atividades de pesquisa, publicação e divulgação.
Como jornalista freelancer, escreve sobre temas relacionados a direitos de quarta geração, novas tecnologias e segurança da informação.

Lista degli articoli
Visita il sito web dell’autore