

A Lei Geral de Proteção de Dados Pessoais (LGPD) é de suma importância na proteção dos dados pessoais sensíveis.

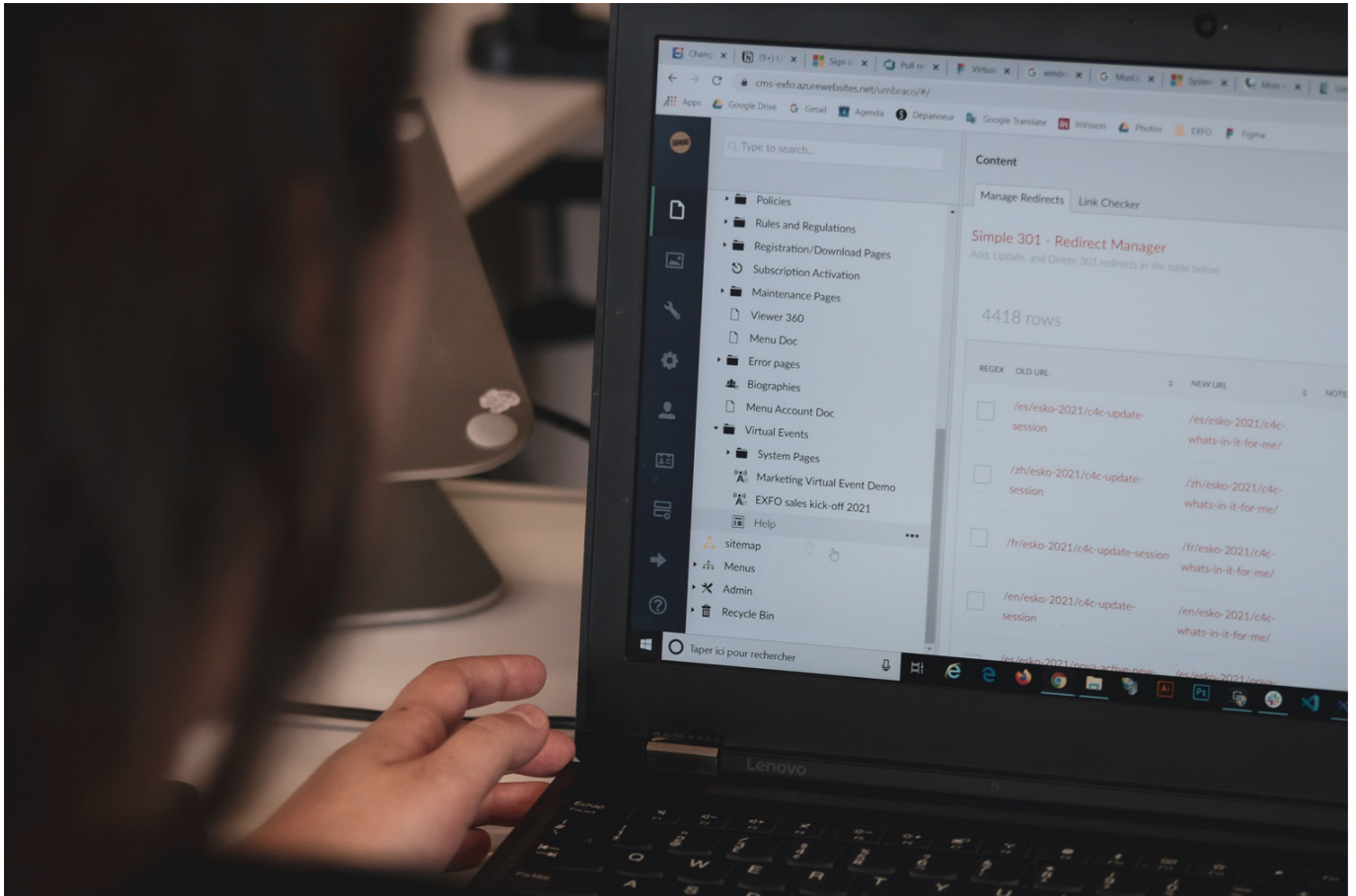
Essa relevância na proteção dos **dados pessoais sensíveis** decorre, principalmente, do caráter discriminatório que tais dados podem suscitar, prejudicando seus titulares, [quando expostos de maneira indevida](#).

De modo geral, os dados pessoais sensíveis são dados pessoais relativos à origem racial ou étnica, religião, política, dados relativos à saúde ou vida sexual e dados biométricos, quando relacionados a uma pessoa física.

Como o Brasil tem mais de 138 milhões de usuários de internet, tornando-se o maior mercado de Internet da América Latina e o quarto maior do mundo, há uma grande chance de que sua organização precise cumprir a LGPD.

O legislativo brasileiro projetou a LGPD para alcançar um acordo de adequação com a UE para garantir um livre fluxo de dados entre os dois.

COMO A LGPD IMPACTA NA SEGURANÇA CIBERNÉTICA?



A LGPD exige que os controladores e processadores adotem medidas técnicas e administrativas para proteger os dados pessoais.

Essas medidas visam a proteção contra **acessos não autorizados**, destruição acidental ou legal, perda, alteração e exposição, principalmente no tocante aos dados sensíveis.

Nesse sentido, a possibilidade de que as organizações possam ser responsabilizadas pelas ações de fornecedores terceirizados, é outra razão pela qual o gerenciamento de riscos de fornecedores está se tornando mais importante.

Por isso, a LGPD impacta diretamente na segurança cibernética de uma empresa.

Nesse viés, para que a segurança cibernética seja completamente garantida, é preciso que a empresa compreenda, em sua maioria, os termos definidos pela LGPD.

Estes termos serão apresentados abaixo.

QUAIS SÃO OS TERMOS DEFINIDOS NA LGPD?

Além dos dados pessoais sensíveis, o artigo 5º da LGPD tem outras 18 definições:

- **Dados pessoais:** Informações sobre uma pessoa natural identificada ou identificável semelhante a informações pessoalmente identificáveis (PII).
- **Dados anonimizados:** Dados relacionados a um sujeito de dados que não pode ser identificado por meio do uso de meios técnicos razoáveis e disponíveis no momento do processamento.
- **Base de dados:** Conjunto de dados pessoais estruturados e mantidos em um ou vários locais, com suporte físico ou eletrônico.
- **Titular:** Uma pessoa natural a quem os dados pessoais que são objeto de processamento referem-se.
- **Controlador:** Pessoa física ou jurídica, de direito público ou privado, que tenha competência para tomar as decisões relativas ao [processamento de dados pessoais](#).
- **Processador:** Pessoa física ou jurídica, de direito público ou privado, que processa dados pessoais em nome do controlador.
- **Encarregado:** Pessoa apontada pelo controlador, que atua como um canal de comunicação entre o controlador e os sujeitos de dados e a **autoridade nacional**.
- **Agentes de tratamento:** O controlador e o processador.
- **Tratamento:** Qualquer operação realizada com dados pessoais.

Entre outros termos como anonimização, consentimento, bloqueio, eliminação, transferência internacional de dados, uso compartilhado de dados, relatório de impacto à proteção de dados pessoais, órgão de pesquisa e autoridade nacional.

Em conclusão, estas são algumas ponderações acerca dos **dados pessoais sensíveis**. Gostou do conteúdo e quer saber mais informações sobre o universo do Direito Digital? [Continue acompanhando nosso blog e siga nosso Instagram para mais conteúdos.](#)