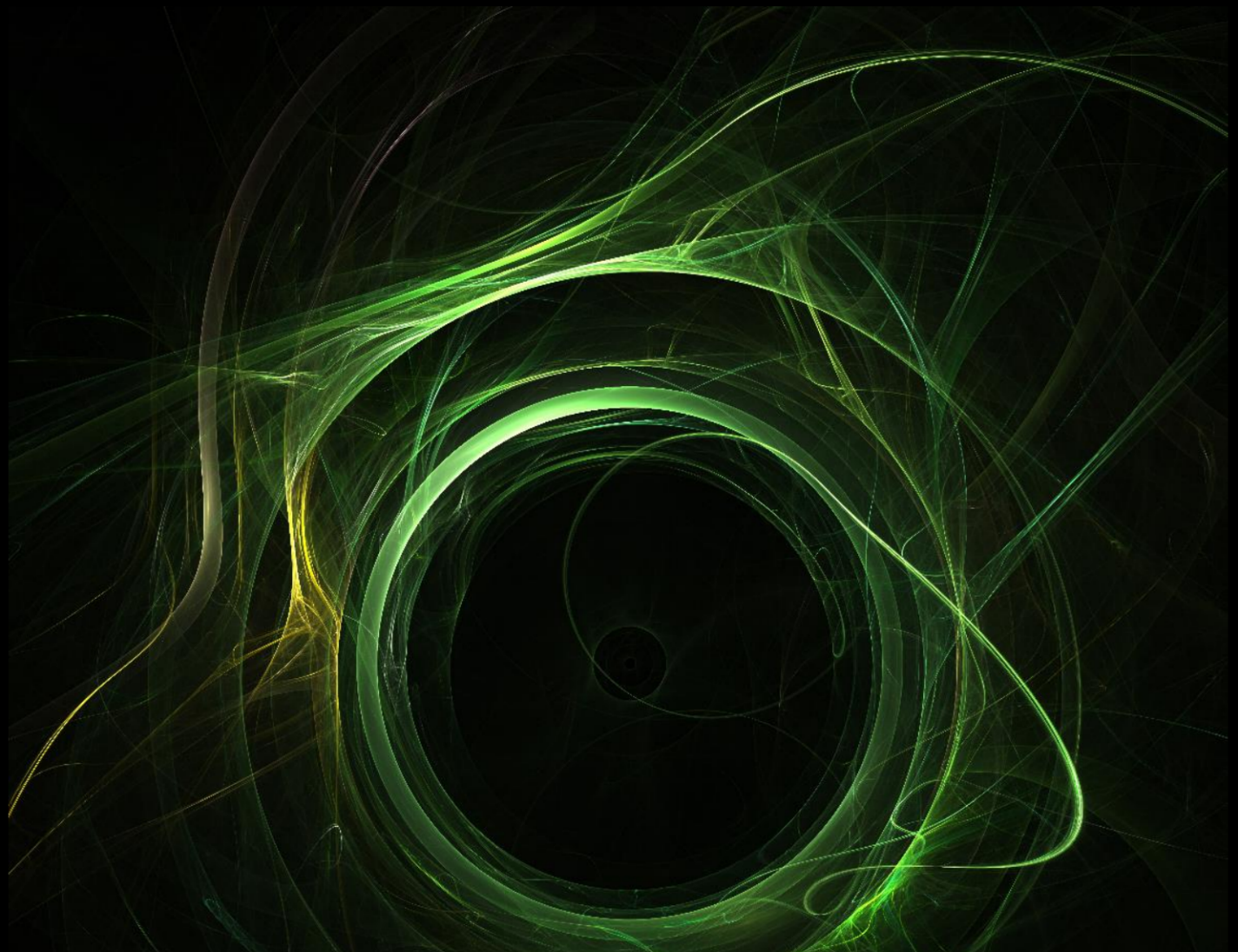
Deloitte.



Aspectos Práticos LGPD e IA

Palestra realizada na Câmara de Comércio e Indústria Japonesa do Brasil em 15.05.2024

Agenda

1. Contexto regulatório atual
2. Proteção de Dados e IA
3. Gestão de Incidentes

1 Contexto regulatório atual

Contexto atual regulatório de proteção de dados no Brasil

Contexto regulatório

LGPD

Em vigor desde set/2020.

Regulamento Incidentes

Em abril/2024, a ANPD publicou Resolução CD/ANPD que aprova o **Regulamento de Comunicação de Incidente de Segurança**

Consulta pública

Em abril/2024, a ANPD abriu consulta sobre **tratamento de dados pessoais de alto risco**

IA

ANPD apresenta propostas de alteração do substitutivo ao **PL 2338**, sobre inteligência artificial

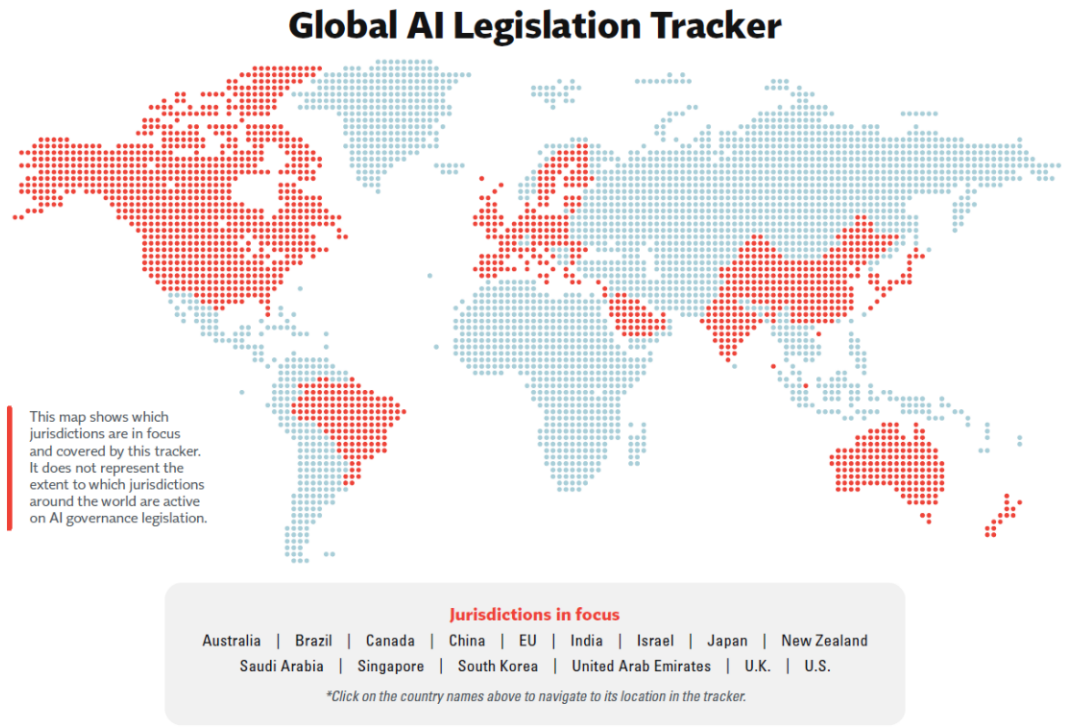
2

Proteção de Dados e IA

Conectando 2 mundos

Panorama da IA no Brasil e no Mundo

Deloitte.



Global AI Legislation Tracker • International Association of Privacy Professionals • iapp.org

No Brasil:

O Brasil possui cerca 46 projetos de lei para regulamentar o uso da IA;

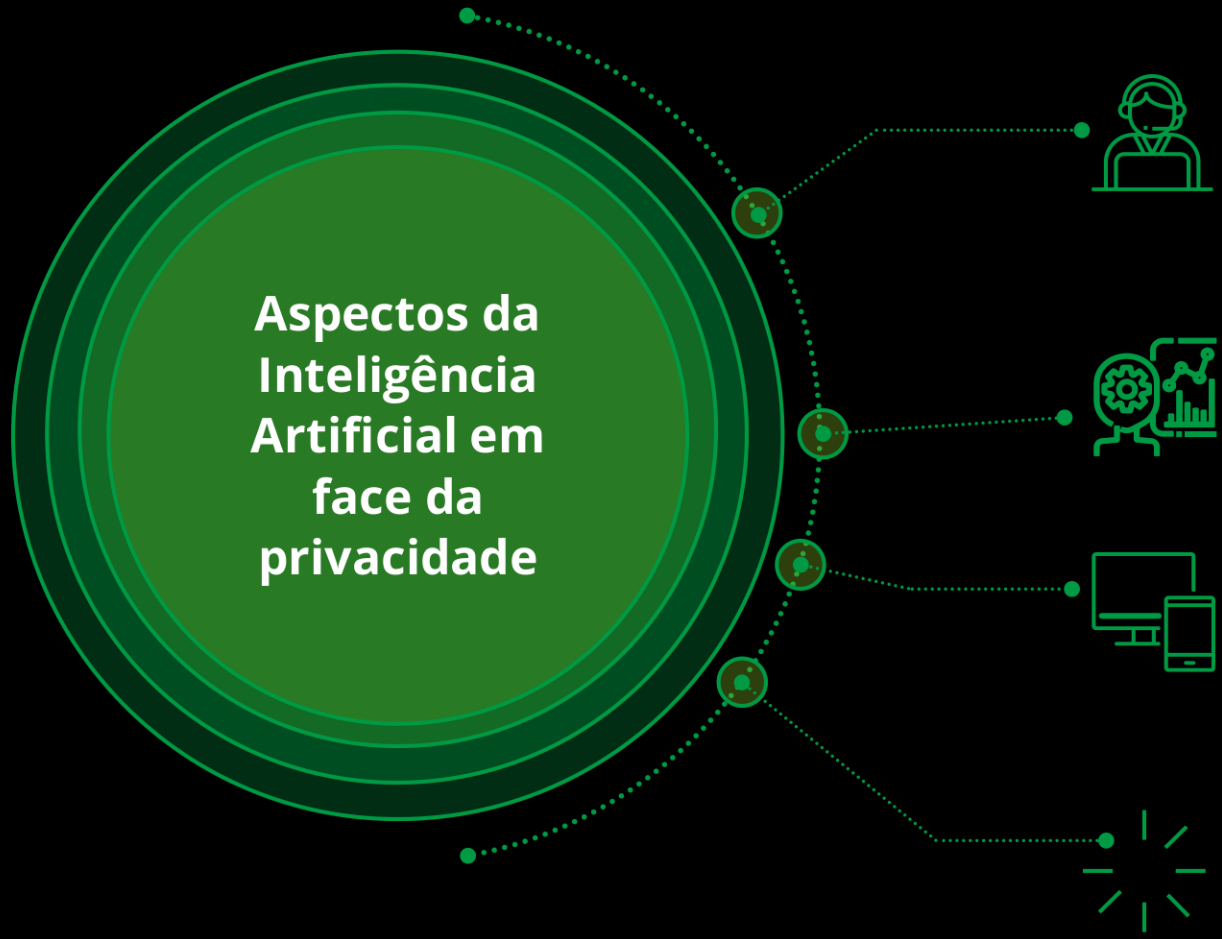
PL 2338/23 é o mais avançado e estabelece balizas para o desenvolvimento e a aplicação da IA.

No mundo:

Países	Abordagem regulatória
Austrália	Não existe lei, mas o Governo já ressaltou a importância regulatória da IA.
Canada	Projeto de lei em tramitação para proteger os cidadãos dos sistemas de alto risco.
China	A China é um dos primeiros países a implementar regulamentações de IA
UE	A EU está finalizando a aprovação regulatória de IA.
Índia	Não existe lei, mas o Governo já ressaltou a importância regulatória da IA.
Israel	Projeto de lei em tramitação, o país possui iniciativas de governança.
Japão	Não existe lei, mas o Governo já ressaltou a importância regulatória da IA.
Nova Zelândia	Não existe lei, mas possui agência regulatória de impactos algorítmicos.
Arábia Saudita	Não existe lei, mas está na agenda regulatória do país.
Singapura	Não existe lei, mas o país possui iniciativas de governança.
Coréia do Sul	O país está atuando através de outras leis para regulamentar a governança de IA.
Emirados Árabes	Não existe lei, mas está na agenda regulatória do país, além das iniciativas governamentais.
Reino Unido	O país está atuando através de outras leis para regulamentar a governança de IA junto com orientações políticas.
EUA	Os Estados Unidos não possuem uma regulamentação abrangente para inteligência artificial, mas existem inúmeros frameworks, diretrizes e instituições governamentais.

Privacidade e IA: conectando os dois mundos da tecnologia digital

A Inteligência Artificial depende de grandes conjuntos de dados para funcionar, o que pode levar à violação da privacidade, caso os dados pessoais processados não forem tratados com a devida governança



Privacy by Design

Garantir a privacidade como parte integrante do desenvolvimento de sistemas de IA, minimizar a coleta e o uso de dados pessoais e Implementar medidas de segurança e proteção de dados desde o início da criação da tecnologia.

Security by Design

Implementar medidas de segurança robustas para proteger os dados contra violações e adotar medidas para prevenir ataques cibernéticos.

Decisões automatizadas

Garantir a transparência dos algoritmos de IA e suas decisões, assegurar o direito à explicação e contestação de decisões automatizadas, consoante a LGPD.

Viéses algorítmicos

Identificar e mitigar os vieses presentes nos dados e algoritmos de IA, assegurar que a IA não perpetue discriminações existentes em conformidade com os princípios da LGPD.

3 Gestão de Incidentes

Programa de Privacidade & Segurança da Informação

O QUE É UM INCIDENTE?

Um incidente de segurança é um evento adverso que impacte ao menos um dos pilares centrais da segurança da informação (confidencialidade, integridade e disponibilidade) dos dados pessoais tratados pelo controlador.

A ANPD também incluiu nesses pilares a autenticidade

Confidencialidade
Acesso somente por pessoas autorizadas

Integridade
Informações não modificadas ou destruídas

Disponibilidade
Imediatamente acessíveis

Autenticidade
Legitimidade, autêntico

O QUE É PRECISO COMUNICAR?

Devem ser comunicados incidentes de segurança confirmados que envolvam dados pessoais e que possam acarretar risco ou dano relevante aos titulares de dados.

4 elementos fundamentais que devem estar presentes para que surja aos controladores de dados o dever de comunicação previsto na LGPD:

(i) a existência de um incidente de segurança;

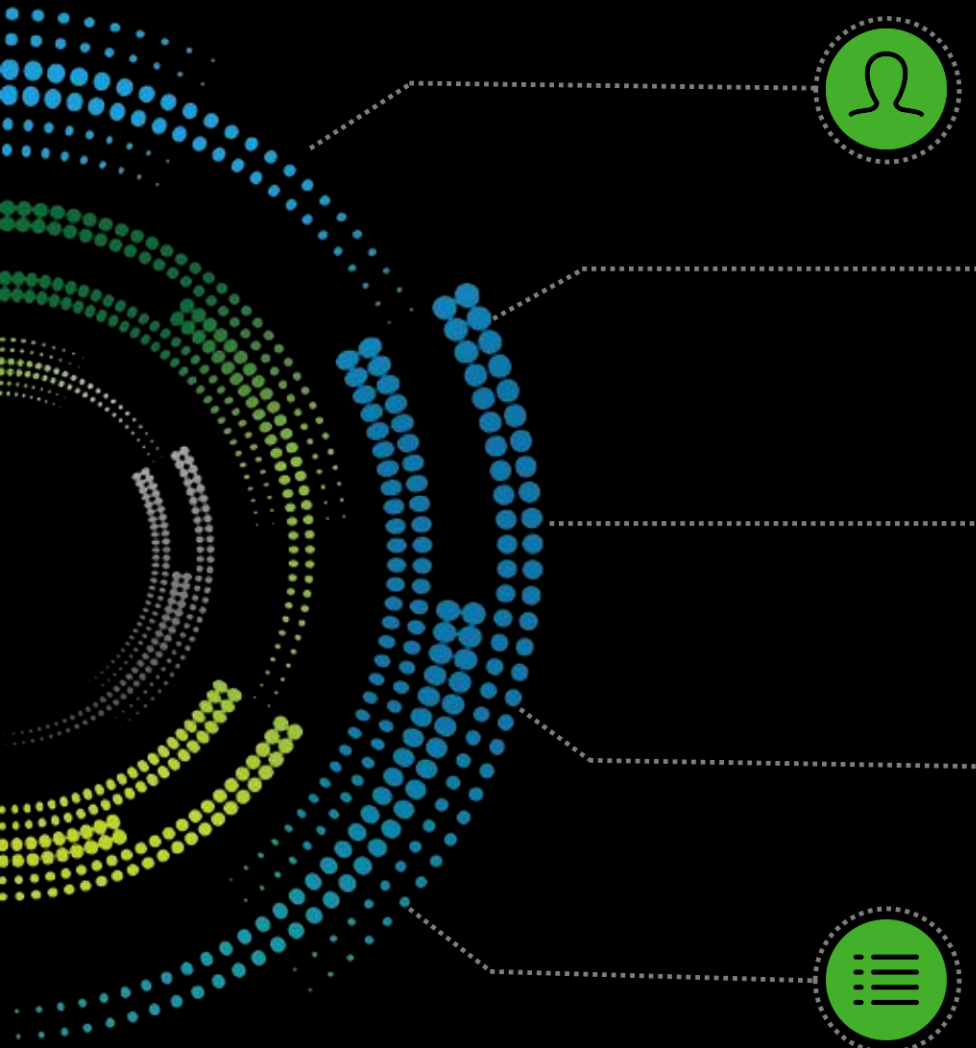
(ii) que seja confirmado;

(iii) que envolva dados pessoais;

(iv) a possibilidade de ocasionar riscos ou danos relevantes aos titulares

Na visão da ANPD, podem acarretar riscos ou danos relevantes incidentes de segurança que tiverem potencial de afetar significativamente interesses e direitos fundamentais e que envolverem ao menos um dos seguintes critérios: (i) dados pessoais sensíveis; (ii) dados de crianças, de adolescentes ou de idosos; (iii) dados financeiros; (iv) dados de autenticação em sistemas; (v) dados protegidos por sigilo legal, judicial ou profissional; ou (vi) dados em larga escala.

COMO COMUNICAR?



A comunicação deve ser realizada em até 3 dias úteis, contados da data do conhecimento do incidente.

O prazo é aplicável tanto para a comunicação à ANPD, quanto para a comunicação aos titulares.

A comunicação aos titulares deve ocorrer de forma direta e individualizada.

A comunicação à ANPD deve ser realizada por meio de formulário disponibilizado pela Autoridade, a ser protocolado eletronicamente pelo SUPER.BR (Sistema Único de Processo Eletrônico em Rede).

A comunicação pode ser complementada com informações adicionais no prazo de 20 dias úteis, contados da data da comunicação anterior, de maneira fundamentada

Mitigação de risco em privacy

Governança em P&PD

Estruturação de uma **governança em privacidade e proteção de dados pessoais** são essenciais para uma abordagem estratégica e eficiente voltada ao gerenciamento de riscos.

Estratégias de Cyber

Promoção de **estratégias de *cyber*** como forma de prevenção e/ou repressão a incidentes de segurança da informação envolvendo dados pessoais.

DICAS PRÁTICAS

Seguem algumas sugestões a partir da nossa experiência na condução de incidentes de dados:

(i) É fundamental ter um plano de gestão de incidentes que reflita o nível de maturidade da empresa, seja conhecido e praticado por todos, especialmente os gestores;

(ii) É essencial que se realizem simulações de incidentes de dados (analogia SIPA);

(iii) Planos de continuidade de negócios e recuperação de desastres são fundamentais também e precisam dialogar com o plano de gestão de incidentes;

(iv) Não espere para contratar fornecedores no momento do incidente (empresas de investigação forense; assessoria de imprensa, etc.); não haverá tempo e isso pode impactar diretamente na habilidade da empresa de gerir bem o incidente;

(v) Revise sua apólice de seguro cibernético;

(vi) Envolva o seu DPO;

(vii) Faça uma gestão crítica do tempo a partir do momento em que surge a suspeita do incidente;

(viii) Nem todo incidente deve ser reportado, mas todo incidente deve ser registrado em relatório que poderá, inclusive, ser requisitado pela ANPD.

CONTATO

Sócio de Privacy

Telefone: (11) 91469-5733

Deloitte.