ASPECTOS INTRODUTÓRIOS:

IMPORTÂNCIA DA DATA PROTECTION

Prof. Iuri Pinheiro

Caso ifood

BREVE DEMONSTRAÇÃO SOBRE A IMPORTÂNCIA DA *DATA PROTECTION*

✓ Aspectos concorrenciais

- caso *ifood:* "Como apps de entrega estão levando pequenos restaurantes à falência" www.bbc.com/portuguese/geral-51272233
- caso *Target:* monitoramento dos padrões de comportamento para enviesamento

2222
target
we're hiring.
we're hiring.
TARGET

BREVE DEMONSTRAÇÃO SOBRE A IMPORTÂNCIA DA *DATA PROTECTION*

- **Caso Target:**
  mulher de 23 anos levou para casa uma *loção de manteiga de coco, uma bolsa grande o suficiente para guardar fraldas, suplementos como zinco e magnésio e um tapete azul, há 87% de chance de ela estar esperando um bebê há 3 meses*.

PASSAGENS AÉREAS

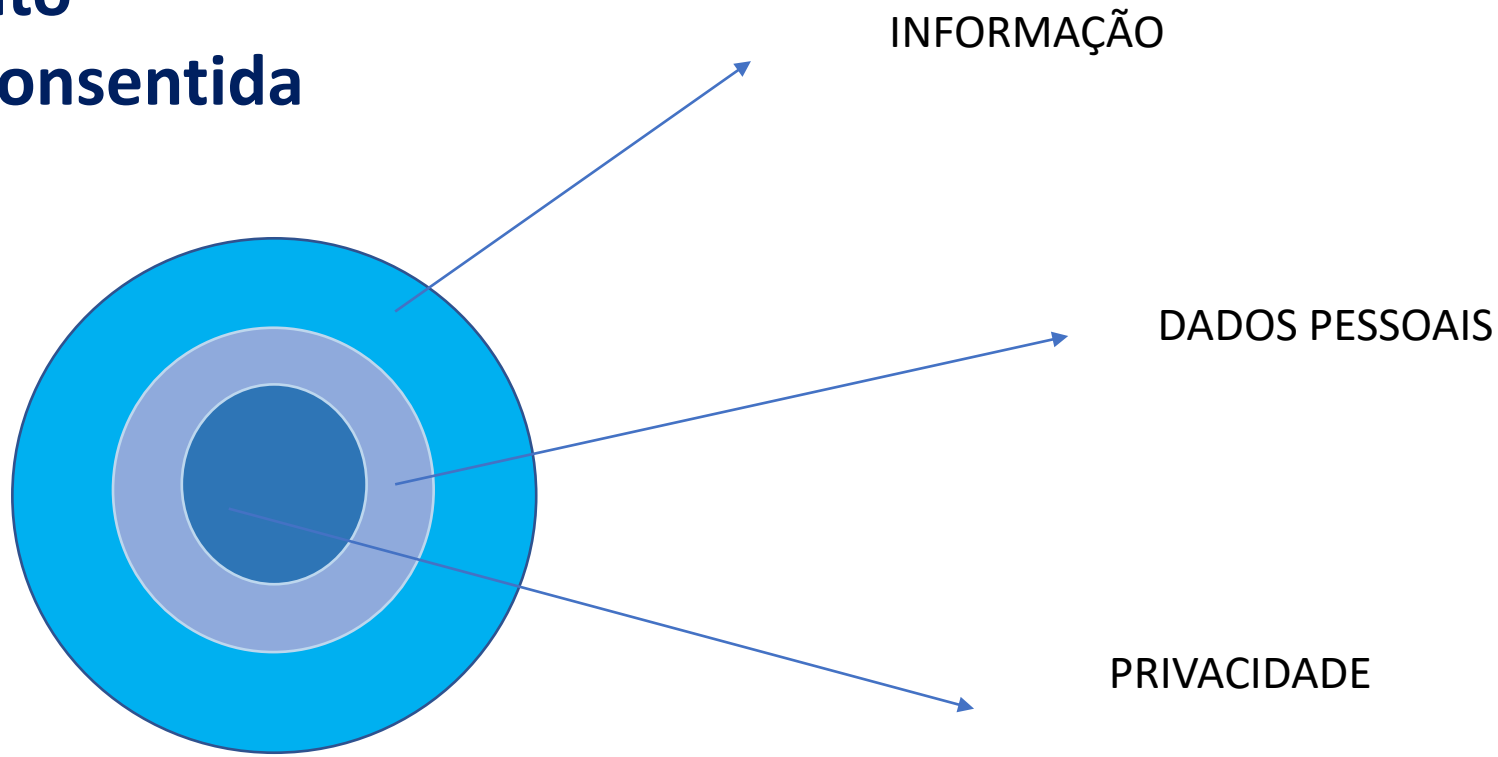
BREVE DEMONSTRAÇÃO SOBRE A IMPORTÂNCIA DA *DATA PROTECTION*

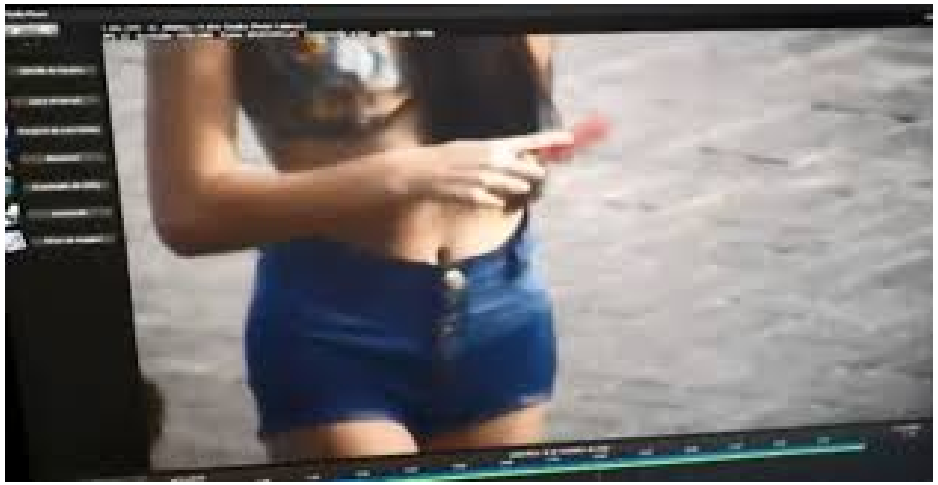
- **Impacto na tomada de decisões empresariais na relação comercial com consumidores.**

- Exemplo: oferta de passagens aéreas com base na localização geográfica do cidadão, prática conhecida como ***geopricing* (precificação geográfica). Exemplo:** acesso o site http://www.moovin.com.br/ e veja a oferta de "Sistema Multi-preços", consistente na possibilidade aplicar ***preços diferentes para um mesmo produto*** conforme a origem de acesso (comparadores de preço e campanhas de marketing).

INFORMAÇÃO RETIRADA DE DADOS PESSOAIS X PRIVACIDADE

Antes – Anonimato
Hoje – exibição consentida





DESVIRTUAMENTO

Servidores aproximam imagens de câmeras da Prefeitura de Guaratuba para ver mulheres na praia

Procuradoria do município disse que vai investigar; outros funcionários denunciaram o caso depois que procuraram por imagens de um garoto desaparecido e não encontraram.

O jovem **suspeito de chefiar um esquema que desviou R$ 400 milhões** de contas bancárias abriu mão dos bens milionários para cumprir prisão domiciliar. Pablo Henrique Borges, de 24 anos, aceitou um acordo e disse que vai colaborar com as investigações.

Ad was inappropriate
Not interested in this ad
Seen this ad multiple times
Ad covered content

O rapaz, que foi preso na **Operação Ostentação** na semana passada, ficou apenas dois dias na carceragem do Departamento Estadual de Investigações Criminais (Deic), na Zona Norte de São Paulo. Na noite de sexta (12) ele já estava em casa.

Hackers podem atacar roteadores de internet para redirecionar sites e roubar senhas; saiba se proteger

Para Anatel e Procon, consumidor pode pedir troca de equipamentos cedidos por provedores que não mais receberem atualizações de segurança dos fabricantes.

DESVIRTUAMENTO

Deu Tilt #1: Não é lenda! Hackers roubam centavos de bancos até ter milhões

Hackers atacam milhares de sistemas corporativos através de vulnerabilidade

Analistas de malware dizem que ataque é executado através de aplicativos ASP.NET que usam a estrutura Telerik

NOTÍCIAS E REFLEXÕES

Cada 1 dólar investido em privacidade pode render 3,30 às empresas

Site para "infiéis" Ashley Madison é atacado; dados de 37 milhões de usuários podem ser expostos

Por Emerson Alecrim
4 anos atrás

NEWS

Cambridge Analytica vai encerrar operações após escândalo com o Facebook

Netshoes paga R$ 500 mil em danos morais após vazamento de dados

Netshoes faz acordo com MPDFT para evitar ação coletiva; empresa sofreu vazamentos de dados em 2017 e 2018

NASA descobre vazamento de dados que comprometeu antigos e atuais funcionários

Amazon demite funcionários por vazar dados de clientes para terceiros

OUTRAS FONTES MATERIAIS E FUNDAMENTOS

DADO PESSOAL É O PRINCIPAL INSUMO DA ECONOMIA GLOBALIZADA E BASEADA NA TECNOLIGIA

ECONOMIA DIRIGIDA POR DADOS – DATA DRIVEN ECONOMY

FALTA DE COMPETITIVIDADE DAS EMPRESAS QUE NÃO SE ADEQUARAM

DESRESPEITO À DEMOCRACIA (eleição do Trump)

DESRESPEITO À DIREITOS FUNDAMENTAIS (Amazon)

QUAIS SÃO AS FONTES MATERIAIS DA *LGPD*?

- ***"Por que tanta importância atribuída à necessidade de um marco regulatório de proteção de dados?***

  A resposta, porém, é simples: o dado pessoal é, hoje, o **principal insumo da economia** globalizada e baseada em tecnologia.

  Cada vez mais, dados são processados e valorados economicamente. Afinal, vivemos a era da economia dirigida por dados" ***(data driven economy)***

A controvérsia dos 50 milhões de perfis do Facebook manipulados pela Cambridge Analytica

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades

Vazamento sem precedentes expôs dados de 50 milhões de usuários e mergulhou empresa em nova crise, pouco tempo depois de comoção sobre disseminação de notícias falsas

Facebook ainda é evasivo sobre Cambridge Analytica e fake news

Comitê digital e de mídia do Reino Unido está examinando notícias falsas e dados obtidos de forma inadequada por consultoria da campanha de Trump

BREVE DEMONSTRAÇÃO SOBRE A IMPORTÂNCIA DA *DATA PROTECTION*

✓ Defesa da democracia

- caso *Cambridge Analytica:* vazamentos de dados do Facebook a uma companhia que trabalhou na campanha da eleição de Trump. Esse material foi utilizado em conjunto com algoritmos, para criar um conjunto de ações para influenciar eleitores nos Estados Unidos e em vários outros países — em especial no pleito estadunidense de 2016 e no plebiscito sobre o Brexit.

amazon

BREVE DEMONSTRAÇÃO SOBRE A IMPORTÂNCIA DA *DATA PROTECTION*

- ✓ **Proteção de direitos fundamentais, especialmente no contexto laboral**
  - caso *Amazon 1: "Amazon rastreia produtividade dos trabalhadores e os dispensa por isso"*. Fonte: www.olhardigital.com.br/noticia/amazon-rastreia-produtividade-dos-trabalhadores-e-os-dispensa-por-isso/85218

BREVE DEMONSTRAÇÃO SOBRE A IMPORTÂNCIA DA *DATA PROTECTION*

- ✓ **Proteção de direitos fundamentais, especialmente no contexto laboral**
  - caso *Amazon 2: "Amazon desiste de ferramenta secreta de recrutamento que mostrou viés contra mulheres: a equipe vinha criando programas de computador desde 2014 para revisar os currículos dos candidatos a emprego, com o objetivo de automatizar a busca por talentos".*

amazon

ASPECTOS INTRODUTÓRIOS:

FASES LEGISLATIVAS DA PROTEÇÃO DE DADOS NO BRASIL

LEI 13.709/18
(14/08/2018)

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

FASES LEGISLATIVAS SOBRE *DATA PROTECTION* NO BRASIL

- Fases da legislação *infraconstitucional:*

  a) Fase de **anomia** infraconstitucional

  b) Fase **legislativa** *(principais...)*

     – Lei nº 8.078, de 11.10.1990 (***CDC***) **(arts. 43 a 45)**
     – Lei nº 9.507, de 12.11.1997 **(*Habeas Data*)**
     – Lei nº 12.414, de 9.06.2011 **(*Cadastro Positivo*)**
     – Lei nº 12.527, de 18.11.2011 **(*LAI*)**
     – Lei nº 12.965, de 23.04.2014 (***Marco Civil da Internet***)
     – Lei nº 13.709, de 14.08.2018 *(**LGDP**)*

AMERICA DO NORTE
EUROPA
ASIA
OCEANO PACIFICO
AMERICA CENTRAL
AMERICA DO SUL
OCEANO ATLÂNTICO
AFRICA
OCEANO INDICO
OCEANO PACIFICO
OCEANIA
ANTARTIDA

EUROPA

GDPR - Vigor desde maio de 2018 – exige proteção de dados transferidos internacionalmente

BRASIL (Um dos últimos) para não perder a concorrência

FONTE DE INSPIRAÇÃO NO DIREITO COMPARADO: *GDPR*

- **1973:** O Conselho da Europa já disciplina juridicamente o tratamento de dados pessoais desde 1973, por meio da Resolução nº 22 de 1973 e da Resolução nº 29 de 1974, ambas versando sobre princípios para proteção de informações pessoais em bancos de dados automatizados, tanto no setor público, como privado.

- **1981:** *Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais* – Convenção nº 108, do Conselho da Europa – considerado o primeiro instrumento internacional disciplinando especificamente o assunto com força legal, aberta inclusive a países não membros da Comunidade Europeia.

FONTE DE INSPIRAÇÃO NO DIREITO COMPARADO: *GDPR*

- **1995:** editada a Diretiva nº 46, recentemente sucedida pelo Regulamento Geral de Proteção de Dados (***GDPR***, em sua sigla em inglês), que entrou em vigor no dia 25 de maio de 2018.

- **2018: entra em vigor a GDPR**

ASPECTOS INTRODUTÓRIOS:

POR QUE AS EMPRESAS DEVEM SE ADEQUAR À LGPD?

POR QUE AS EMPRESAS DEVEM SE ADEQUAR À LGPD?

- **Tendência de mercado** (**agregar valor à marca** e à **empresa**, **maior transparência** e **controle de informações** etc);

- A GDPR (25.05.2018) **aplica-se também a todas as empresas** que tratam dados pessoais de indivíduos que se encontram em **território europeu** no momento da coleta ou que ofereçam serviços à sua população;

POR QUE AS EMPRESAS DEVEM SE ADEQUAR À LGPD?

- Empresas europeias ficaram praticamente **impedidas de contratar** com empresas situadas em países que não dispõe do nível de proteção adequado, o que incluía o Brasil ("**isolamento**" que diminuía a competitividade das empresas brasileiras no cenário internacional - *Ferraço*)
- Trata-se de um **obrigação legal**, com pesadíssimas **multas** e riscos de responsabilidade civil (*passivo*) (multas de até 2% do faturamento da empresa, limitado a R$ 50 milhões) e bloqueio ou eliminação dos dados relacionados a uma infração.

POR QUE AS EMPRESAS DEVEM SE ADEQUAR À LGPD?

Penalidades Administrativas (art. 52)

Responsabilidade civil Moral e patrimonial (art. 42)

POR QUE AS EMPRESAS DEVEM SE ADEQUAR À LGPD?

Penalidades Administrativas (art. 52): Os ***agentes de tratamento*** de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - **advertência**, com indicação de prazo para adoção de medidas corretivas;

II - **multa simples**, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

POR QUE AS EMPRESAS DEVERÃO SE ADEQUAR À LGPD?

III - **multa diária**, observado o limite total a que se refere o inciso II;

IV - **publicização da infração** [...];

V - **bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;

VI - **eliminação dos dados pessoais** a que se refere a infração;

POR QUE AS EMPRESAS DEVERÃO SE ADEQUAR À LGPD?

X - **suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - **suspensão do exercício da atividade de tratamento dos dados** pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - **proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados**.

FONTES MATERIAIS:

FATORES SOCIAIS, ECONÔMICOS, HISTÓRICOS ETC QUE LEVARAM À EDIÇÃO DA LGPD

FONTES MATERIAIS

QUAIS SÃO AS FONTES MATERIAIS DA *LGPD*?

- Notícias relevantes sobre casos de **vazamento** ou **uso indevido** de dados pessoais na imprensa nacional ou internacional (vide, por exemplo, caso de manipulação eleitoral e política – *Cambridge Analytica*)

- Necessidade de **adequação** aos padrões mundiais (No total, cerca de 125 países no mundo já adotaram normas específicas de proteção e dados, o que revela a grande adesão global à questão, dos quais **6, na América do Sul**: Chile, Argentina, Uruguai, Paraguai, Peru e Colômbia.

QUAIS SÃO AS FONTES MATERIAIS DA *LGPD*?

- Constantes **violações** aos direitos fundamentais de privacidade e intimidade dos indivíduos;
- Risco de **isolamento** do mercado e perda da competitividade das empresas nacionais, aliado à perda de **investimentos** estrangeiros etc (razão *econômica*)

QUAIS SÃO AS FONTES MATERIAIS DA *LGPD*?

- Trecho do relatório dos PLs nºs: **53/2018 (Câmara)**; **330/13** e **181/2014 (Senado)**; **131/2014**, autoria da Comissão Parlamentar de Inquérito da Espionagem (CPIDAESP), os quais tramitaram em conjunto.

  "A despeito do contexto de crise econômica, é seguro afirmar que o País tem perdido oportunidades valiosas de investimento financeiro internacional em razão do isolamento jurídico em que se encontra por não dispor de uma lei geral e nacional de proteção de dados pessoais (LGPD)" (Senador Ricardo Ferraço)

POR QUE AS EMPRESAS DEVERÃO SE ADEQUAR À LGPD?

*"O dado pessoal é hoje **insumo** principal da atividade econômica em todos os setores possíveis da sociedade. É, ainda, como já afirmamos, elemento fundamental até mesmo para a concretização de políticas públicas, dado o elevado grau de informatização e sistematização do Estado brasileiro, em todos os níveis federativos. Mais que isso: o dado pessoal é um ingrediente indissociável da **privacidade** do cidadão e sua preservação guarda conformidade com o efetivo respeito a **garantias fundamentais do indivíduo**, tal como prescritas na Constituição federal."* (Senador Ricardo Ferraço)

Quais são os objetivos da LGPD?

- Direito à privacidade: garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando garantir direitos e liberdades fundamentais.

- Regras claras paras as empresas: estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para as empresas.

- Promover o desenvolvimento: fomentar o desenvolvimento econômico e tecnológico em uma sociedade *data driven.*

Quais são os objetivos da LGPD?

- Direito do consumidor: garantir a livre a iniciativa, a livre concorrência e a defesa do consumidor.

- Fortalecer a confiança: aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais.

- Segurança jurídica: aumentar a segurança jurídica como um todo no uso e tratamento de dados pessoais.

Vantagens da adoção de proteção de dados:

- Adequar as regras no Brasil: tornar o nosso país apto para processar dados oriundos de outros países que exigem um nível de proteção adequado, o que pode fomentar, principalmente, os setores de tecnologia da informação.

- Portabilidade: sujeitos poderão transferir seus dados de um serviço para outro, aumentado a competitividade no mercado.

Vantagens da adoção de proteção de dados:

- Unificação de regras: regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia.

- Maior flexibilidade: autorizar formas mais flexíveis para o tratamento dos dados pessoais, tais como legítimos interesses, que levam em consideração uma sociedade movida a dados em tempos de Big Data.

- Redução de custos: diminuir os custos operacionais causados por incompatibilidades sistêmicas de tratamentos feitos por agentes diversos, além de fomentar uma maior qualidade dos dados em circulação no escossistema como um todo.

ÁREAS IMPACTADAS

Áreas impactadas:

- Análise de dados
- Marketing
- Desenvolvimento de software e tecnologia da informação
- Gerenciamento de produtos
- Jurídico
- Compliance
- Recursos Humanos
- Serviços e logística
- Segurança da informação

FUNDAMENTOS JUSTRABALHISTAS INFRACONSTITUCIONAIS

Princípio da proteção na CLT: art. 444, CLT → relação assimétrica: poder empregatício vs. direitos fundamentais relação assimétrica → incapacidade do trabalhador de salvaguadar seus direitos fundamentais → limites e contornos à autonomia privada → lugares impenetráveis pelo empregador → a realidade laboral deseja e admite o controle do empregador de determinados aspectos da rotina laboral (aumento da segurança e saúde, produtividade etc.) → limite à entradas abusivas → direito fundamental à reserva/proteção da intimidade e vida privada e à *autodeterminação informativa* → hipóteses de tratamento de dados.

Art. 2º, A disciplina da proteção de dados pessoais tem como FUNDAMENTOS:

I Respeito à privacidade

II Autodeterminação informativa

III Liberdade de expressão, informação, comunicação e opinião

IV Inviolabilidade da intimidade, honra e imagem

V Desenvolvimento econômico e tecnológico e à inovação

VI Livre iniciativa, concorrência e a defesa do consumidor

VII Direitos humanos, livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais.

CONCEITOS BÁSICOS

Art. 5º – Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural *identificada* ou *identificável*;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

A lei não conceitua dado sensível. O rol é exemplificativo ou taxativo? O que no futuro vai permitir classificar/segregar a pessoa? A ANPD terá a importante missão de mencionar outras hipóteses, até porque ela tem como papel a interpretação da lei, nos termos da própria LGPD.

CONCEITOS BÁSICOS

III - <u>dado anonimizado</u>: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

> ***Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei**, <u>salvo</u> quando o processo de anonimização ao qual foram submetidos **<u>for revertido</u>**, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, **<u>puder ser revertido</u>**.*
>
> *§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.*
>
> *§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.*
>
> *§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.*

CONCEITOS BÁSICOS

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais *um dado perde a* ***possibilidade de associação****, direta ou indireta, a um indivíduo;*

[ANONIMIZAÇÃO]

DADOS COLETADOS:

(ANTES DA ANONIMIZAÇÃO)

NOME: GISELE KAUER

GÊNERO: FEMININO

NACIONALIDADE: BRASILEIRA

PROFISSÃO: ADVOGADA

OAB/SP: 430.653

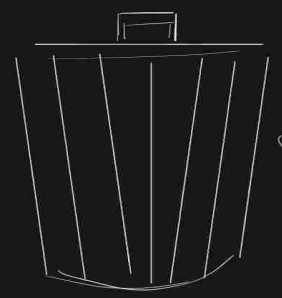
→ ANONIMIZAÇÃO →

DADOS ANONIMIZADOS:

GÊNERO: FEMININO

NACIONALIDADE: BRASILEIRA

PROFISSÃO: ADVOGADA



GISELE KAUER

SP (SEÇÃO DA OAB)

430.653

O QUE ACONTECE AQUI?

SÃO ELIMINADOS OU DESASSOCIADOS DADOS QUE POSSAM IDENTIFICAR UM TITULAR.

- EXCLUSÃO PERMANENTE -

(SEM POSSIBILIDADE DE RECUPERAÇÃO | RESTAURAÇÃO)

(OU DESASSOCIAÇÃO ATRAVÉS DE MEIOS TÉCNICOS RAZOÁVEIS PRÓPRIOS)

CONCEITOS BÁSICOS

Anonimização vs. pseudonimização

Art. 13, § 4º se refere à ***pseudonimização*** como o tratamento por meio do qual um dado *perde a possibilidade de associação, direta ou indireta*, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

A definição é bem semelhante à trazida pelo ***GDPR***: é o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

[PSEUDONIMIZAÇÃO]

DADOS COLETADOS:

(ANTES DA PSEUDONIMIZAÇÃO)

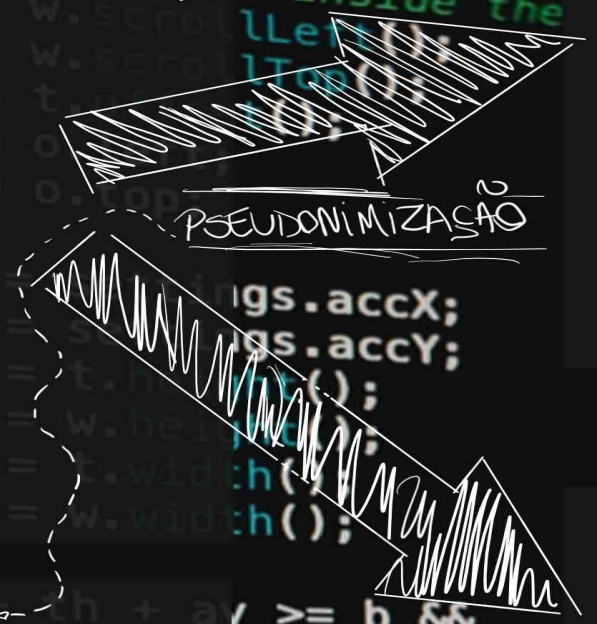
NOME: GISELE KAUER

GÊNERO: FEMININO

NACIONALIDADE: BRASILEIRA

PROFISSÃO: ADVOGADA

OAB/SP: 430.653



BANCO DE DADOS #1

DADOS PSEUDONIMIZADOS:

GÊNERO: FEMININO

NACIONALIDADE: BRASILEIRA

PROFISSÃO: ADVOGADA

IDENTIFICADOR: 1066204

O QUE ACONTECE AQUI?

IDENTIFICADORES DIRETOS

(EX.: NOME, RG, CPF, PASSAPORTE, TELEFONE)

SÃO MANTIDOS SEPARADAMENTE!

(ATRAVÉS DE MEDIDAS TÉCNICAS E ADMINISTRATIVAS)

BANCO DE DADOS #2

(CONTENDO IDENTIFICADORES)

ID: 1066204

NOME: GISELE KAUER

OAB/SP: 430.653

OBJETO E SUJEITOS DA LGPD

Eficácia subjetiva

(arts. 1º e 4º da LGPD)

OBJETO DE REGULAÇÃO e SUJEITOS

Artigo 1º – Esta Lei dispõe sobre o *tratamento* de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o *objetivo* de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As *normas gerais* contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

OBJETO DE REGULAÇÃO e SUJEITOS

O que é tratamento de dados?

Art. 5º *Para os fins desta Lei, considera-se: [...]* ***X - tratamento:*** *toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;*

OBJETO DE REGULAÇÃO e SUJEITOS

OBJETO DE REGULAÇÃO e SUJEITOS

Indivíduo
(empregado-titular dos dados)

Pessoa jurídica

Direito Privado

Direito Público

Pessoa Natural

OBJETO DE REGULAÇÃO e SUJEITOS

Em quais situações de tratamento a LGPD não se aplica?

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins ***exclusivamente particulares*** e ***não econômicos;***

- ✓ ***Aplica-se às relações de trabalho doméstico?***

OBJETO DE REGULAÇÃO e SUJEITOS

Em quais situações de tratamento a LGPD não se aplica?

Art. 4º [...] II - realizado para fins exclusivamente: *a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;*

OBJETO DE REGULAÇÃO e SUJEITOS

Em quais situações de tratamento a LGPD não se aplica?

Art. 4º [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;

§ 1º [...] será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

OBJETO DE REGULAÇÃO e SUJEITOS

Em quais situações de tratamento a LGPD não se aplica?

Art. 4º [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;

§ 2º É **vedado** o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

FUNDAMENTOS

(art. 2º da LGPD)

CONCEITOS BÁSICOS

Art. 5º – Para os fins desta Lei, considera-se:

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

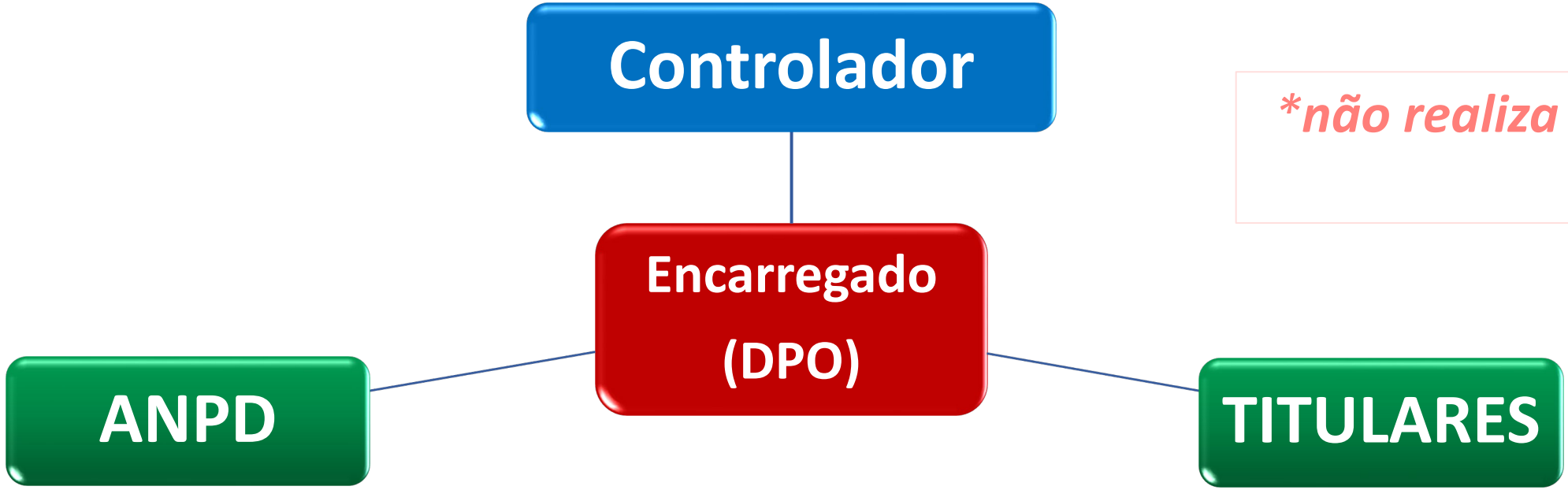
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as ***decisões*** referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o ***tratamento*** de dados pessoais em nome do controlador;

CONCEITOS BÁSICOS

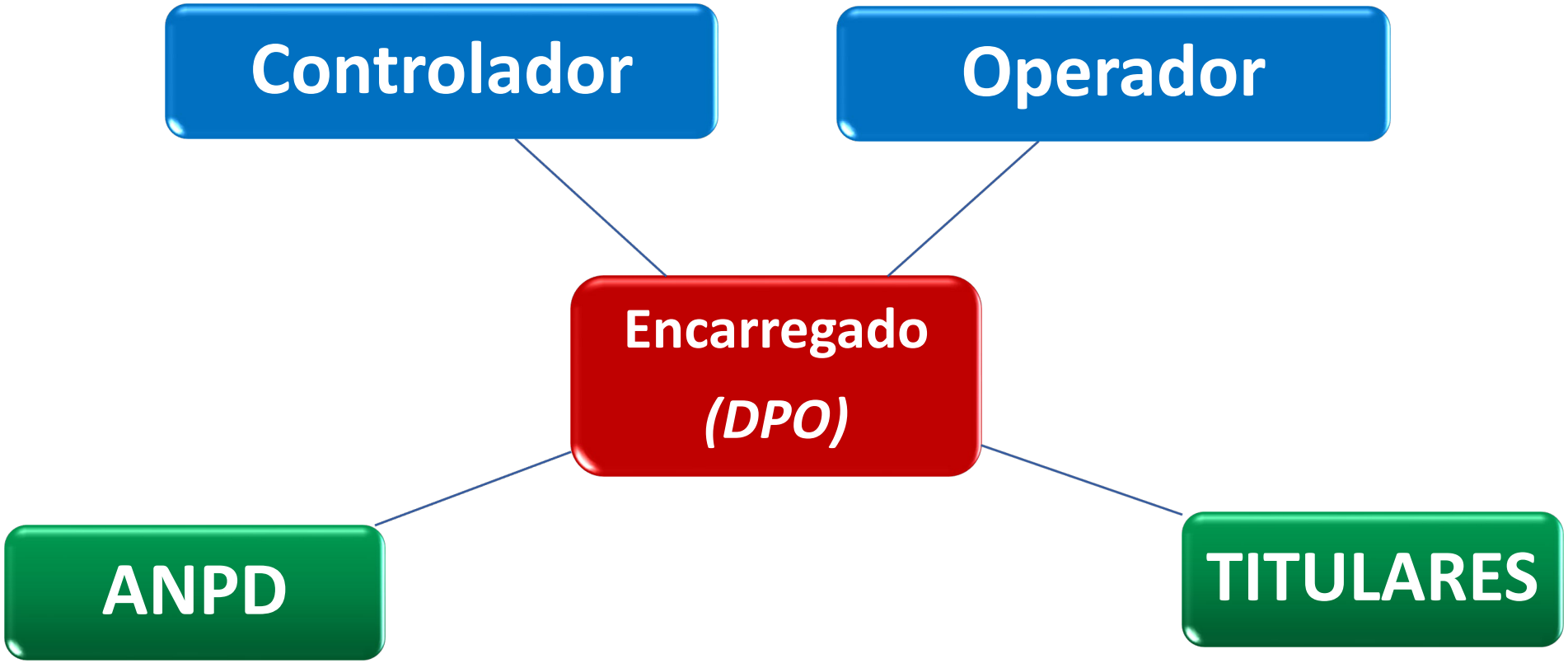
VIII – <u>encarregado*</u>: pessoa indicada pelo controlador e operador para atuar como **<u>canal de comunicação</u>** entre o **<u>controlador</u>**, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)



**não realiza tratamento de dados*

CONCEITOS BÁSICOS

IX - <u>agentes de tratamento</u>: o controlador e o operador;



CONCEITOS BÁSICOS

X - <u>tratamento</u>: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

CONCEITOS BÁSICOS

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais *um dado perde a **possibilidade de associação**, direta ou indireta, a um indivíduo;*

XII - consentimento: manifestação **livre**, **informada** e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma ***finalidade determinada***; **(*não precisa ser expresso, nem se forem dados sensíveis*: "[...] consentir, de forma *específica* e *destacada*, para finalidades específicas".**

CONCEITOS BÁSICOS

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

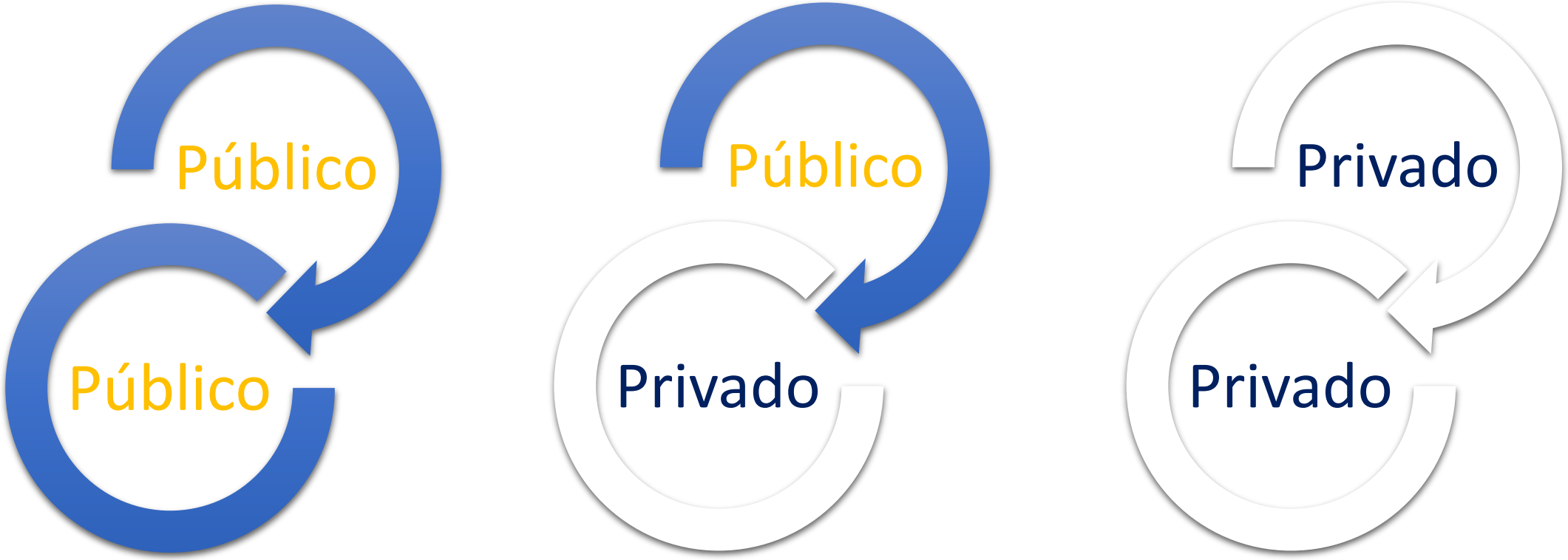
XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

CONCEITOS BÁSICOS

XVI - <u>uso compartilhado de dados</u>: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, ***reciprocamente***, com ***autorização específica***, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou *entre entes privados*;

CONCEITOS BÁSICOS – *Uso compartilhado de dados*



CONCEITOS BÁSICOS

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que **podem gerar riscos** às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de **mitigação de risco**;

CONCEITOS BÁSICOS

XVIII - <u>órgão de pesquisa</u>: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado **sem fins lucrativos** legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

CONCEITOS BÁSICOS

XIX - <u>autoridade nacional</u>: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

PRINCÍPIOS

(art. 6º da LGPD)

OS 10 PRINCÍPIOS PARA O TRATAMENTO DE DADOS DE ACORDO COM A LGPD

1 FINALIDADE

Apenas coletar dados pessoais para fins legítimos, informando com clareza o usuário a finalidade da coleta

2 ADEQUAÇÃO

Disponibilizar todas as informações sobre a coleta e uso de dados para o usuário de forma honesta

3 NECESSIDADE

Manter e utilizar apenas os dados essenciais, apagando-os quando deixarem de ser relevantes

4 LIVRE ACESSO

Ser capaz de apresentar ao usuário os dados e a forma como são processados ao ser requisitado

5 PRECISÃO

Manter os dados precisos a todo o momento, deletando ou atualizando dados errados ou imprecisos

6 TRANSPARÊNCIA

O usuário deve ser informado de maneira clara e acessível sobre os riscos e direitos sobre seus dados

7 SEGURANÇA

Tomar medidas técnicas e administrativas para proteger os dados de danos, furtos ou perdas

8 PREVENÇÃO

Tomar medidas preventivas para a proteção dos dados, evitando danos aos titulares

9 NÃO DISCRIMINAÇÃO

Não utilizar os dados para nenhum fim discriminatório, ilícito ou abusivo, atendendo aos requisitos de lei

10 RESPONSABILIDADE

Adotar estes princípios e ter condições de provar sua adoção em todos os procedimentos da empresa

WSI

PRINCÍPIOS

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - <u>finalidade</u>: realização do tratamento para **propósitos legítimos**, **específicos**, **explícitos** e **informados** ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

II - adequação: compatibilidade do tratamento *com as finalidades informadas* ao titular, de acordo com o contexto do tratamento;

PRINCÍPIOS

*Exemplos práticos no DT dos princípios da **finalidade** e **adequação**:*

- ✓ *sistemas de vídeo monitoramento para segurança e aplicação de penalidades;*
- ✓ *dados de candidatos a empregos e envio futuro de publicidade;*
- ✓ *tratamento de dados de forma oculta e monitoramento do Linkedin p/ fiscalizar cumprimento de cláusulas de não concorrência.*

PRINCÍPIOS

III – necessidade (*minimização*): limitação do tratamento **ao mínimo necessário** para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

PRINCÍPIOS

Por quanto <u>tempo</u> o empregador poderá armazenar os dados?

- Princípio da necessidade e tempo de registro: limitação do tratamento ao mínimo necessário em relação às finalidades do tratamento de dados.

- Premissas sobre a prescrição: **<u>efeito</u>** (extinção da pretensão), **<u>conceito</u>** (ato-fato-jurídico caducificante, pois encobre a eficácia) e **<u>requisitos</u>** (inércia do titular da pretensão + decurso do tempo).

PRINCÍPIOS

Por quanto <u>tempo</u> o empregador poderá armazenar os dados?

- ***Marco inicial:*** ciência inequívoca

- ***Candidatos ao emprego:*** 5 anos

- ***Empregados e ex-empregados:*** 5 anos ou 2 anos ou tempo indeterminado (imprescritível) .

PRINCÍPIOS

Por quanto <u>tempo</u> o empregador poderá armazenar os dados?

[...] não há falar em prescrição bienal, pois não houve contrato de trabalho e tampouco rescisão contratual, o que atrai a incidência da prescrição quinquenal. Assim, [...] inexistia relação de emprego, e em se tratando de fase pré-contratual, aplica-se a ***prescrição quinquenal*** do art. 7º, XXIX, da Constituição Federal, incidente às relações de trabalho. [...] (E-ED-RR-AIRR-173400-24.2008.5.02.0445, SDI-1, Relator Ministro Aloysio Correa da Veiga, DEJT 11/04/2017).

PRINCÍPIOS

IV - livre acesso: garantia, aos titulares, de consulta facilitada e *gratuita* sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

PRINCÍPIOS

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

"*As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future*" **(ARTICLE 29 WORKING PARTY OPINION ON THE PROCESSING OF PERSONAL DATA IN THE EMPLOYMENT CONTEXT)**

PRINCÍPIOS

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

PRINCÍPIOS

VIII - prevenção: adoção de medidas para *prevenir* a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

REQUISITOS PARA O TRATAMENTO DE DADOS NÃO SENSÍVEIS

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de **consentimento** pelo titular;

- o problema do consentimento nas relações assimétricas de poder (relação de trabalho subordinado);
- Dispensa do consentimento (§ 4º, deste art. 7º);
- Compartilhamento posterior ao consentimento;
- Análise do artigo 8º;

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

II – p/ o cumprimento de **obrigação legal** ou **regulatória** pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Cap. IV desta Lei (*Do tratamento de dados pelo Poder Público*);

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a ***anonimização*** dos dados pessoais;

V - quando necessário para a execução de contrato *ou* de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de set. de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos **interesses legítimos do controlador** ou **de terceiro**, **exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais**; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

Exemplo prático de interesse legítimo:

Empregador monitora de forma **não oculta** os perfis de redes sociais de ex-empregados com o intuito de aferir, através do histórico profissional disponibilizado nestas redes, se estes cumprem com as cláusulas de não concorrência ou de confidencialidade constantes dos seus contratos de trabalho, cujas referidas cláusulas continuam em vigor mesmo após a cessação dos respectivos vínculos laborais, a finalidade desse tratamento pode ser entendida como, em abstrato, legítima.

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

Exemplo prático de interesse legítimo:

O tratamento de dados pessoais decorrentes dessa monitorização pode ser fundamentado na necessidade do mesmo para a **tutela dos interesses legítimos** da entidade empregadora – *i. e.*, a não transferência de *know-how*, técnicas e métodos de antigos trabalhadores para empresas diretamente concorrentes com a atividade por esta exercida – desde que tal monitorização seja realizada da forma **menos intrusiva possível**. (LUIS, João Vares; HENRIQUES, Sérgio Coimbra. *Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral*. In: *Anuário da proteção de dados 2019*. Lisboa: Universidade Nova de Lisboa, 2019, p. 32)

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

Exemplo prático de interesse legítimo:

O GT29 aponta exemplo concreto sobre o tema: "Um empregador monitoriza os perfis de antigos empregados no LinkedIn que estão envolvidos durante a vigência das cláusulas de não concorrência. A finalidade desta monitorização consiste em controlar a conformidade com essas cláusulas. A monitorização é limitada a estes antigos empregados. **Enquanto o empregador puder provar que tal monitorização é necessária para proteger os seus interesses legítimos, que não existem outros meios menos invasivos disponíveis e que os antigos empregados tenham sido devidamente informados da extensão da observação regular das suas comunicações públicas, o empregador pode invocar o fundamento jurídico do art. 7.º, alínea f), da Diretiva"** (cfr. ponto 5.2 do Parecer 2/2017 do GT29).

LEGÍTIMO INTERESSE DO CONTROLADOR (Art. 7º, inc. *IX*)

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

LEGÍTIMO INTERESSE DO CONTROLADOR

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS:

Ônus da prova

Toda estrutura da LGPD conduz ao entendimento de que recai sobre as entidades empregadoras o ônus de assegurar e comprovar que se encontram aptas a demonstrarem que tomaram as medidas adequadas a garantir o necessário equilíbrio entre a prossecução de uma finalidade (legítima) de tratamento de dados e o respeito pelas liberdades e direitos fundamentais dos trabalhadores e as expectativas razoáveis destes na relação com as suas entidades empregadoras.

TRATAMENTO DE DADOS PESSOAIS CUJO ACESSO É PÚBLICO

§ § 1ºe 2º - Revogados

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

DISPENSA DO CONSENTIMENTO

§ 4º É **dispensada a exigência do *consentimento*** previsto no *caput* deste artigo para os **dados tornados manifestamente públicos pelo titular**, resguardados os direitos do titular e os princípios previstos nesta Lei.

CONSENTIMENTO ESPECÍFICO PARA COMPARTILHAMENTO DE DADOS

§ 5º O controlador que obteve o consentimento referido no inciso I do *caput* deste artigo que necessitar **comunicar** ou **compartilhar** dados pessoais com outros controladores deverá obter **consentimento específico** do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

DISPENSA DO CONSENTIMENTO E DEMAIS OBRIGAÇÕES

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

TRATAMENTO POSTERIOR DADOS PESSOAIS PÚBLICOS

§ 7º O tratamento **posterior** dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

A FORMA COMO DEVE SE DAR O CONSENTIMENTO

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido **por escrito** ou por **outro meio** que demonstre a **manifestação de vontade** do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de **cláusula destacada** das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

A FORMA COMO DEVE SE DAR O CONSENTIMENTO

Para o GT29, exemplos de consentimentos explícitos são:

(i) Confirmação do consentimento por meio de uma declaração por escrito;
(ii) Assinatura de uma declaração escrita;
(iii) Envio de declaração por meio do preenchimento de um formulário eletrônico;
(iv) Envio de declaração por e-mail;
(v) Envio de um documento assinado digitalizado;
(vi) Usando uma assinatura eletrônica.

AUTORIZAÇÃO GENÉRICA PARA O TRATAMENTO

§ 4º O consentimento deverá referir-se a **finalidades determinadas**, e as **autorizações genéricas** para o tratamento de dados pessoais **serão nulas**.

REVOGAÇÃO DO CONSENTIMENTO: *TEMPO E MODO*

§ 5º O consentimento pode ser **revogado a qualquer momento** mediante *manifestação* *expressa* do titular, por procedimento gratuito e facilitado, *ratificados* os tratamentos realizados sob amparo do consentimento anteriormente manifestado ***enquanto não houver requerimento de eliminação***, nos termos do inc. VI do *caput* do art. 18 desta Lei.

ALTERAÇÕES QUANTO TRAMENTO DE DADOS JÁ COLHIDOS

§ 6º Em caso de alteração de informação referida nos incisos **I (finalidade específica do tratamento), II (forma e duração do tratamento)**, **III (identificação do controlador)** ou **V (informações acerca do uso compartilhado de dados pelo controlador e a finalidade)** do art. 9º desta Lei, o controlador deverá informar ao titular, com **destaque de forma específica do teor das alterações**, podendo o titular, nos casos em que o seu consentimento é exigido, ***revogá-lo*** caso discorde da alteração.

PRINCÍPIO DO LIVRE ACESSO

Art. 9º O titular tem direito ao **acesso facilitado** às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do **princípio do livre acesso**:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

ACESSO AOS DADOS PESSOAIS PELO TITULAR

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

NULIDADE DO CONSENTIMENTO

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado **nulo** caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas *previamente* com transparência, de forma clara e inequívoca.

MUDANÇAS DA FINALIDADE INCOMPATÍVEIS COM O CONSENTIMENTO ORIGINAL

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais **não compatíveis com o consentimento original**, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

FORNECIMENTO DE DADOS COMO CONDIÇÃO P/ O FORNECIMENTO DE PRODUTO/SERVIÇO OU P/ EXERCÍCIO DE DIREITO

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será **informado com destaque** sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

REQUISITOS PARA O TRATAMENTO DE DADOS SENSÍVEIS

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Art. 11. O tratamento de dados pessoais **sensíveis** somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma ***específica*** e ***destacada***, para finalidades específicas;

II - **sem fornecimento de consentimento** do titular, nas hipóteses em que for *indispensável* para:

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) **exercício regular de direitos, inclusive *em contrato*** e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do *caput* deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis ***referentes à saúde com objetivo de obter vantagem econômica***, **exceto nas hipóteses relativas a <u>prestação de serviços de saúde</u>, <u>de assistência farmacêutica</u> e <u>de</u> <u>assistência à saúde</u>**, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

§ 5º É **vedado** às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a **prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários**. (Incluído pela Lei nº 13.853, de 2019)

TESTE BARBALESCU (BARBALESCU VS ROMÊNIA)

Corte Europeia de Direitos Humanos

i) grau de intromissão do empregador;
ii) existência de uma razão empresarial para justificar o controle;
iii)inexistência de outros meios menos intrusivos para consecução do mesmo objetivo;
iv) destinação dada pela empresa aos resultados do controle; e,
v) previsão de garantias ao trabalhador.